IBM Directory Server

Installation and Configuration Guide

Version 5.1

IBM Directory Server

Installation and Configuration Guide

Version 5.1

Note

Before using this information and the product it supports, read the general information under Appendix I, "Notices" on page 145.

First Edition (November 2002)

This edition applies to version 5, release 1, of the IBM® Directory Server and to all subsequent releases and modifications until otherwise indicated in new editions.

Preface

This document describes how to install, configure, and remove the IBM Directory Server version 5.1. IBM Directory Server 5.1 is supported on Windows®, Linux (Intel), Linux for S/390, AIX®, Hewlett-Packard UNIX® (HP-UX), and Solaris operating system platforms. For detailed information about supported operating system versions, as well as other required software and hardware, see Chapter 2, "System requirements" on page 5.

What's new for this release

The following enhancements and changes have been made to IBM Directory Server for the 5.1 release.

New Web Administration Tool

A new graphical user interface (GUI) called the Web Administration Tool is provided in this release for administering servers. This tool incorporates the function previously in the Directory Management Tool (DMT), which has been removed. Many of the product enhancements, such as replication improvements and password policy enhancements, can be exploited through the Web Administration Tool. In addition, a simple interface for user and group administration, which does not require LDAP expertise, is included in the Web Administration Tool.

The Web Administration Tool is installed as a separate package that does not require installation of the server or the client software. You can install the Web Administration Tool on a computer that is used to administer servers remotely. An application server, which is required to use the tool, can be installed with the Web Administration Tool.

New configuration tools

The IBM Directory Server Configuration Tool, **ldapxcfg**, has been updated to contain all functions that must be performed locally on a server. The Configuration Tool is a GUI. You can now use the Configuration Tool for the following tasks on a local server:

- Set or change the administrator distinguished name (DN) and password
- Configure or unconfigure the database
- Enable or disable the change log
- Add or remove a suffix
- Add a schema file to or remove a schema file from the list of schema files to be loaded at startup
- Import or export LDIF data
- Back up, restore, or optimize the database

In addition, the command line utilities **ldapcfg** and **ldapucfg** have been updated. The **ldapcfg** utility can be used for many of the tasks that the Configuration Tool performs. The **ldapucfg** utility can be used to unconfigure the database. The **dbback**, **dbrestore**, and **runstats** utilities are provided for backing up, restoring, and optimizing the database. For more information, see Chapter 10, "Configuration" on page 63.

Replication improvements

Replication has been enhanced to include the following functions:

Cascaded replication
Cascaded replication is now supported. A cascading replication is a replication topology in which there are multiple tiers of servers. A peer/master server replicates to a small set of read-only servers which in turn replicate to other servers. Such a topology offloads replication work from the master servers.

Subtree replication
Replication can now be configured for individual subtrees of the directory.

Administrative GUI to correct replication errors
The Web Administration Tool now shows the current state of the replication queues and indicates any problem conditions. The administrator can then make corrective changes to the replication queue so that replication can proceed. For example, the administrator can delete a failing update from the queue, so that the updates that follow it can be processed.

Administrative GUI for topology changes
The Web Administration Tool now shows the entire current replication topology. The administrator can add replicas to the topology and promote replicas to forwarding replicas or masters. The administrator can make some topology changes (for example, addition of new replicas) without restarting any of the servers in the topology. Other topology changes (for example, promotion of a replica to a forwarding replica) might require a restart.

Scheduled replication
When you configure a replication target, you can now specify particular times of the day at which you want replication to occur.

Access controls based on filter
This feature provides for a new form of access control information. A comparison filter can be specified to determine the target of an access control list (ACL). The filter is applied to the entry where the ACL is defined, plus all descendent entries. The ACL is applied to any entries that match the filter at the time access is being determined. For example, this feature might be used to grant write access for an individual to all entries matching the filter "(objectclass=cimPrinter)". If a new printer definition is added to the subtree, this individual (in effect, a printer administrator) automatically has write access, based on subsequent evaluations of the search filter in the ACL.

Protection of access control information
This feature limits access to the access control information in the directory. In previous releases, anyone who had read access to an entry could also read the ACLs for that entry, but only an entry owner or the administrator DN could update an ACL. In this release, an option is provided so that users who cannot update the ACLs also cannot read the ACLs. The other option is for ACL access to remain as it was in previous releases. This can be set through the Web Administration Tool.

Password policy
This feature provides for a set of configurable policy rules to be applied to user passwords in the directory. The following functions are provided:

Login failure lockout
If a user unsuccessfully attempts to log in a number of times in a

row, the user is blocked until either a timeout expires or an administrator intervenes. The occurrence of lockouts is recorded.

Password history
When a user changes a password, the new password is checked against a configurable number of previous passwords to ensure that it has not been used by that user recently.

Password syntax
A policy to enforce the syntax of a password; for example, minimum length or minimum number of numeric characters can be set.

Password expiration
The administrator can configure the directory so that user passwords expire after a certain amount of time. The administrator can also configure the directory to require that users modify their passwords after they are set by the administrator but before performing any other operation.

Directory Service Markup Language (DSML) v 2.0 support
A DSML v2.0 interface to the directory is included with this release. The DSML interface makes directory services available to XML-based applications, cell phones, and Personal Digital Assistants (PDAs). With DSMLv2, LDAP requests and responses are expressed as XML document fragments. DSML is installed with the Web Administration Tool.

Performance improvements
IBM Directory Server 5.1 provides improved performance over previous releases.

Updated version (8.1) of DB2®
The installation program includes an integrated installation of DB2 Universal Database version 8.1 Workgroup Server Edition (DB2).

Network Authentication Services (Kerberos) 1.3
The IBM Directory Server C client and server now use the Network Authentication 1.3 C client on AIX. The 64-bit AIX client now supports Kerberos authentication with the Network Authentication Services 1.3 64-bit client.

Accessibility
The Web Administration Tool meets the IBM corporate instruction that makes product offerings accessible to people with disabilities. For the documents, use the HTML, rather than the PDF versions.

IPv6 support on AIX
Both the client and server for AIX are enabled to support IPv6. IPv6 uses a wider address (128-bit vs 32-bit) than IPv4, and this has an impact on the TCP application level. The format of LDAP URLs for IPv4 and IPv6 is as follows:

- To use a literal IPv4 address in a URL, the format is *x.x.x.x:port*. An example of an LDAP server name in a URL is **ldap://9.53.90.21:80**.
- To comply with RFC 2732, literal IPv6 address in URLs must be enclosed in **[** and **]** characters. Examples of LDAP server names in URLs are:
  - ldap://[107:0:0:0:200:7051]:80
  - ldap://[::ffff:9.53.96.21]

Updated version (6.0.3) of GSKit
The installation program now includes an integrated installation of GSKit version 6.0.3.

GB18030 support
Support has been added for code page GB18030 on platforms for which the operating system has added GB18030 support.

New Directory Administration Daemon
The Directory Administration Daemon enables remote management of the IBM Directory Server. It should run at all times on the computer where the IBM Directory Server is installed. The Directory Administration Daemon accepts requests via LDAP extended operations and supports starting, stopping, restarting and status monitoring of the IBM Directory Server. By default, the Directory Administration Daemon listens on two ports: port 3538 for non-SSL connections and port 3539 for SSL connections, if SSL communication is enabled.

Changes to file names

- The slapd executable is named ibmslapd for this release.
- The slapd32.conf configuration file is named ibmslapd.conf for this release.
- The slapd.errors log file is named ibmslapd.log and moved to a new path for this release.
- The cli.error file is named db2cli.log for this release.

New command line utilities
New utilities have been added.

For the client

- **ldapexop** is the LDAP extended operation tool. It provides the capability to bind to a directory and issue a single extended operation along with any data that makes up the extended operation value. It supports the standard host, port, SSL, and authentication options used by all of the LDAP client utilities. In addition, a set of options is defined to specify the operation to be performed and the arguments for each extended operation.
- **ldapchangepwd** is the LDAP modify password tool. It sends modify password requests to an LDAP server.

For the server
ldapdiff is the LDAP replica synchronization tool. It synchronizes a replica server with its master.

Change in processing of attribute type names
The way in which attribute type names are processed and returned to client applications is different in the 5.1 release. The difference is in case sensitivity of the names. The LDAP standards clearly state that attribute type names are case-insensitive, but if you have server plug-ins or applications that depend on the case of the attribute type names, you might need to adjust your program to work with the new release.

- For searches where a specific list of attribute type names is requested, the names returned will match the exact case of the list specified. (Previously, they were always returned in lower case.)

- For searches where no list of attribute type names is requested, the names returned will match the case of the attribute type name used in the schema definition. (Previously, the names were returned in the same form they were entered when that particular entry was added to the directory.)

No default database

In previous releases, a default database was configured. For this release, you must specify the name of the database and the user ID that will own the database. The instance in which the database is created has the same name as the user ID.

Web server no longer required

In previous releases, a Web server was required on the server. A Web server is no longer required.

Contents

Chapter 1. Installation, configuration, and migration overview

This chapter briefly describes the recommended installation, configuration and migration procedures for IBM Directory Server version 5.1.

If you have a pre-existing version of Lightweight Directory Access Protocol (LDAP) from a vendor other than IBM, you must remove it before installing the IBM Directory Server. If you attempt to install the IBM Directory Server without removing the other vendor's version, the resulting file name conflicts might prevent either version from working.

If you have IBM SecureWay® Directory Version 3.1.1.5, 3.2, 3.2.1, or 3.2.2, or IBM Directory Server 4.1 installed and you want to migrate your data, see Chapter 3, "Migration from previous releases" on page 17 before beginning the installation process for the IBM Directory Server 5.1.

Attention: If you have SecureWay Directory Version 3.1.1.5 currently installed and you want to migrate your data, you must upgrade to level 3.2.2 before installing IBM Directory Server 5.1. You can download SecureWay Directory version 3.2.2 from the IBM SecureWay Directory Web site: http://www-4.ibm.com/software/network/directory/downloads/. See the SecureWay Directory version 3.2.2 documentation for information about migrating from version 3.1.1.5.

Before you install: zip, tar, and iso files

The IBM Directory Server product is available in three file formats: zip, tar, and iso.

If you downloaded a zip file, use a product such as PKZIP to unzip the file after you download it to your computer.

The tar file is a Tape ARchive type of file. After you download a tar file, untar it.

The iso version of the product is used to burn an installation CD-ROM that can then be used in the installation process. The iso file is an image that must be processed through a CD-ROM burner program to make the CD-ROM. When you create the CD-ROM, be sure that you do not make a data CD of the iso file. Select the option that unencapsulates the data from the iso file and burns the files on the CD-ROM.

After you process the downloaded file, you can install IBM Directory Server using the installation instructions in the appropriate installation chapter.

Installation

You can install either the IBM Directory Server client or the IBM Directory Server server, which includes the client.

In addition, you can install the new Web Administration Tool on an application server, with or without the server or the client. You use the Web Administration Tool to administer an IBM Directory Server server either locally or remotely. You can install a single Web Administration console to manage multiple IBM Directory Server 5.1 servers.

IBM Directory Server 5.1 has several installation options. You can install using an InstallShield graphical user interface (GUI) or use platform-specific installation methods such as the command line or installation tools for the operating system. Instructions for using the InstallShield GUI are found in Chapter 4, “Installing with the InstallShield GUI” on page 27.

For platform-specific installation instructions, see the installation chapter for the platform for which you are installing. For example, see Chapter 5, “Installing using AIX utilities” on page 39.

Note: The InstallShield GUI installation is not available for HP-UX or Linux for S/390 operating systems.

See Chapter 2, “System requirements” on page 5 for hardware and software prerequisites.

Configuration

You can use either the Configuration Tool (**ldapxcfg**), which has a GUI, or the **ldapcfg** command-line utility to configure the server. To unconfigure the server, you can use **ldapxcfg** or the **ldapucfg** command-line utility.

After successful installation of the server, if you used the InstallShield GUI to install, the Configuration Tool runs. (This is true for all platforms on which the InstallShield GUI is supported.) If you did not use the InstallShield GUI to install, you must run the Configuration Tool or use **ldapcfg**. You must perform the following tasks before you can use the server:

- Set the IBM Directory Server administrator distinguished name (DN) and password. This operation can be compared to defining the root user ID and password on a UNIX system.
- Configure the database.

The **ldapxcfg** program can be used for the following tasks:

- Setting or changing the IBM Directory Server administrator distinguished name (DN) and password
- Configuring and unconfiguring the database
- Enabling and disabling changelog
- Adding or removing suffixes
- Adding schema files to or removing schema files from the list of schema files to be loaded at startup
- Importing and exporting LDIF data
- Backing up, restoring, and optimizing the database

If you prefer to use the command line, all the tasks in the list can be done with a combination of command line utilities, including**ldapcfg**, **ldapucfg**, **dbback**, **dbrestore**, **runstats**, **bulkload**, **ldif2db**, and **db2ldif**.

Instructions for using **ldapxcfg**, **ldapcfg**, **ldapucfg**, **dbback**, **dbrestore**, and **runstats** are found in Chapter 10, “Configuration” on page 63 and Chapter 12, “Unconfiguring the server and uninstalling IBM Directory Server” on page 77.

Migration from a previous release

If you have a previous version of the IBM Directory, such as SecureWay Version 3.1.1.5, 3.2, 3.2.1, or 3.2.2, or IBM Directory Server 4.1, migration is necessary to preserve any changes that you have made to the schema definitions and to preserve your directory server configuration. Use the migration procedures in Chapter 3, “Migration from previous releases” on page 17.

Chapter 2. System requirements

To install the IBM Directory Server packages, administer the server, and use the Global Security Kit (GSKit), your computer must meet the minimum system requirements as outlined in this chapter.

Requirements for the client

The following sections show system requirements for the IBM Directory Server client:

AIX operating system client requirements

Before installing, see the client README file for any updated information about supported versions of the AIX operating system. The file name is client.txt. The file is in the root directory of the CD or the directory where you unzipped or untarred the client package. After installing, the client README file is located in /usr/ldap/web/*lang*/readme/client.txt or /usr/ldap/web/*lang*/readme/client.pdf, or at /usr/ldap/web/*lang*/readme/client.htm for viewing with a Web browser.

lang is the locale you chose when you installed IBM Directory Server.

The following hardware and software are required:

- AIX 4.3.3, 5.1, or 5.2
- A minimum of 128 MB RAM (256 MB is strongly recommended).
- The Korn shell is required.
- In addition to the two filesets required for AIX 4.3.3 you must install AIX Maintenance Level Fix Pack 8 or higher. On AIX 5.1, you must install AIX Maintenance Level Fix Pack 1 or higher.

  Note: If you have no locale-specific requirements, after you apply all the services that you need for your system, restart your system to enable the changes.
- The bos.loc.iso.ZH_TW fileset must be installed for the Taiwan locale. The fileset is available from the AIX 4.3.3 installation medium.
- The xlC.rte 5.0.2.0 or later fileset is required.
- In addition, if you plan to use the InstallShield GUI to install, the following are required for the 32-bit IBM AIX Developer Kit, Java™ Technology Edition, Version 1.3.1 on AIX 4.3.3 and 5.1:
  - For AIX 4.3.3, Java 1.3.1 requires the AIX 4330-09 Recommended Maintenance Level. This maintenance package is intended for customers who already have AIX 4.3.3 installed. The AIX 4330-09 maintenance package can be downloaded from http://techsupport.services.ibm.com/rs6000/fixes/, using APAR number IY22024. If you are a licensee of AIX 4.3.3, you can obtain an Update CD by contacting your point of sale and requesting feature code 0838.
  - For AIX 5.1, Java 1.3.1 requires the AIX 5100-01 Recommended Maintenance Level. This maintenance package is intended for customers who already have AIX 5.1.0 installed. The AIX 5100-01 maintenance package can be downloaded

from http://techsupport.services.ibm.com/rs6000/fixes/, using APAR number IY21957. If you are a licensee of AIX 5.1, you can obtain an Update CD by contacting your point of sale.

Note: Before updating your AIX 5.1.0 system to the AIX 5100-01 maintenance level, you must first apply and commit APAR IY19375 (which includes bos.mp64 5.1.0.1, bos.mp 5.1.0.1, and bos.up 5.1.0.1). Run smitty update and pick IY19375 to install. When the installation completes you must reboot your system. After the system has rebooted, you can then install the AIX 5100-01 maintenance level. After the maintenance level has been installed, you must again reboot. See the AIX 5L™ for POWER Version 5.1 Release Notes™ for more information. APAR IY19375 can be obtained from the AIX Electronic Fix Distribution site: http://techsupport.services.ibm.com/rs6000/fixes/.

If you are using one of the supported non-UTF8 CKJ locales, one of the following filesets (available on both AIX 4.3.3 and AIX 5.1 base CDs) is required:

- X11.fnt.ucs.ttf (for ja_JP or Ja_JP)
- X11.fnt.ucs.ttf_CN (for zh_CN or Zh_CN)
- X11.fnt.ucs.ttf_KR (for ko_KR)
- X11.fnt.ucs.ttf_TW (for zh_TW or Zh_TW)

For Japanese users, if you are using Japanese Input Method, you can apply the following PTFs to avoid some Input Method related problems.

- jkit.Wnn6.base 2.2.0.2 (PTF U479697 or APAR IY22917) (Wnn6 users only)
- X11.motif.lib 5.1.0.15 (PTF U479604 or APAR IY22933) (AIX 5.1 uses only)

Hewlett-Packard UNIX (HP-UX) operating system client requirements

Before installing, see the client README file for any updated information about supported versions of the HP-UX operating system. The file name is client.txt. The file is in the root directory of the CD or the directory where you unzipped or untarred the client package. After installing, the client README file is located in /usr/IBMldap/web/*lang*/readme/client.txt or /usr/IBMldap/web/*lang*/readme/client.pdf, or at /usr/IBMldap/web/*lang*/readme/client.htm for viewing with a Web browser.

lang is the locale you chose when you installed IBM Directory Server.

The following hardware and software are required:

- HP-UX 11i with the following patches:
  - December 2001 GOLDBASE11i bundle
  - December 2001 GOLDAPPS11i bundle
  - patch PHSS_26560
- A minimum of 128 MB RAM. (256 MB is strongly recommended).
- The Korn shell is required.

Linux operating system client requirements

Before installing, see the client README file for any updated information about supported versions of the Linux operating system. The file name is client.txt. The file is in the root directory of the CD or the directory where you unzipped or

untarred the client package. After installing, the client README file is located in /usr/ldap/web/*lang*/readme/client.txt or /usr/ldap/web/*lang*/readme/client.pdf, or at /usr/ldap/web/*lang*/readme/client.htm for viewing with a Web browser.

lang is the locale you chose when you installed IBM Directory Server.

The following hardware and software are required:

- Linux Operating System from Red Hat Version 7.2 or 7.3, Red Hat Linux Advanced Server v2.1, UnitedLinux, or SuSE Version 7.2, 7.3, or 8.0.
- If you are using Secure Sockets Layer (SSL) and GSKit 6.0, you must first download and install the following packages in order:
  1. libgcc-3.0.4-1.i386.rpm
  2. libstdc++3-3.0.1-3.i386.rpm

  You can find these packages at the following Web sites:
  - http://rpmfind.net/linux/RPM/redhat/updates/7.2/i386/libgcc-3.0.4-1.i386.html
  - http://rpmfind.net/linux/RPM/redhat/7.2/i386/libstdc++3-3.0.1-3.i386.html

  For information about GSKit, see "Secure Sockets Layer (SSL) Global Security Kit (GSKit)" on page 15.
- A minimum of 128 MB RAM (256 MB or more is strongly recommended).
- The Korn shell is required.

Linux for S/390 operating system client requirements

Before installing, see the client README file for any updated information about supported versions of the Linux for S/390 operating system. The file name is client.txt. The file is in the root directory of the CD or the directory where you unzipped or untarred the client package. After installing, the client README file is located in /usr/ldap/web/*lang*/readme/client.txt or /usr/ldap/web/*lang*/readme/client.pdf, or at /usr/ldap/web/*lang*/readme/client.htm for viewing with a Web browser.

lang is the locale you chose when you installed IBM Directory Server.

The following hardware and software are required:

- Linux Operating System from Red Hat Version 7.1, SuSE Version 7.0, Turbolinux 6.5.
- A minimum of 128 MB RAM (256 MB or more is strongly recommended).
- The Korn shell is required.

Solaris operating system client requirements

Before installing, see the client README file for any updated information about supported versions of the Solaris operating system. The file name is client.txt. The file is in the root directory of the CD or the directory where you unzipped or untarred the client package. After installing, the client README file is located in /opt/IBMldaps/web/*lang*/readme/client.pdf, or /opt/IBMldaps/web/*lang*/readme/client.htm for viewing with a Web browser.

lang is the locale you chose when you installed IBM Directory Server.

The following hardware and software are required:

- Solaris Operating Environment™ Software versions 7, 8, or 9.
- A minimum of 128 MB RAM. (256 MB is strongly recommended.)
- Ensure that the code page conversion routines (en_US.UTF-8 1.0) are installed.
- The Korn shell is required.
- In addition, if you plan to use the InstallShield GUI to install, patches are required for the Java 2 Runtime Environment, Standard Edition, v. 1.3.1.

  Be sure that you have installed the full set of required patches needed for support of this release. To obtain patches, see the SunSolve support Web site at http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/J2SE. You will find a patch cluster for each Solaris Operating Environment platform. Each patch cluster applies to all supported versions of the Java 2 Standard Edition (J2SE) on the given platform.

  Also see http://java.sun.com/j2se/1.3/font-requirements.html for information about which font packages should be on your system.

  For Solaris 8, patches include:

  – 108652-58 X11 6.4.1: Xsun patch
  – 108921-15 CDE 1.4: dtwm patch
  – 112003-03 SunOS 5.8: Unable to load fontset in 64-bit Solaris 8 iso-1 or iso-15
  – 108773-15 SunOS 5.8: IIIM and X Input & Output Method patch
  – 111293-04 SunOS 5.8: /usr/lib/libdevinfo.so.1 patch
  – 111310-01 SunOS 5.8: /usr/lib/libdhcpagent.so.1 patch
  – 112472-01 SunOS 5.8: Font2DTest2 abort when Lucida Sans Thai Typewriter selected
  – 108714-07 CDE 1.4: libDtWidget patch
  – 111111-03 SunOS 5.8: /usr/bin/nawk patch
  – 112396-02 SunOS 5.8: /usr/bin/fgrep patch
  – 108940-46 Motif 1.2.7 and 2.1.1: Runtime library patch for Solaris 8
  – 108987-09 SunOS 5.8: Patch for patchadd and patchrm
  – 108528-16 SunOS 5.8: kernel update patch
  – 108989-02 SunOS 5.8: /usr/kernel/sys/acctctl and /usr/kernel/sys/exacctsys patch
  – 108827-30 SunOS 5.8: /usr/lib/libthread.so.1 patch

  For Solaris 7, patches include:

  – 107544-03 SunOS 5.7: /usr/lib/fs/ufs/fsck patch
  – 106950-18 SunOS 5.7: Linker Patch
  – 106327-15 32-Bit Shared library patch for C++
  – 106300-16 64-Bit Shared library patch for C++
  – 108376-38 OpenWindows 3.6.1: Xsun Patch
  – 107656-10 OpenWindows 3.6.1 libXt Patch
  – 107702-09 CDE 1.3: dtsession patch
  – 108374-07 CDE 1.3: libDtWidget Patch
  – 107226-18 CDE 1.3: dtwm patch
  – 107081-50 Motif 1.2.7 and 2.1.1: Runtime library patch for Solaris 7
  – 107636-09 SunOS 5.7: X Input & Output Method patch
  – 107153-01 SunOS 5.7: There are three characters missed in zh.GBK songti.ttf

– 107834-03 SunOS 5.7: dkio.h & commands.h patch
– 106541-22 SunOS 5.7: kernel update patch
– 106980-19 SunOS 5.7: libthread patch

Windows 2000, Windows NT, or Windows XP operating systems client requirements

Before installing, see the client README file for any updated information about supported versions of Windows operating systems. The file name is client.txt. The file is in the root directory of the CD or the directory where you unzipped or untarred the client package. After installing, the client README file is located in *installpath*\web*lang*\readme\client.txt or *installpath*\web*lang*\readme\client.pdf, or at *installpath*\web*lang*\readme\client.htm for viewing with a Web browser.

installpath is the location where the IBM Directory Server client is installed.

lang is the locale you chose when you installed IBM Directory Server.

The following hardware and software are required:

- Microsoft® Windows 2000, Windows XP, or Windows NT® 4.0 with Service Pack 6 or higher; a Windows NT file system (NTFS) is required for security support.
- A minimum of 128 MB RAM (256 MB is strongly recommended).

Requirements for the server (including the client)

The following sections show system requirements for installing and using the server, which includes the client:

AIX operating system server requirements

Before installing, see the server README file for any updated information about supported versions of the AIX operating system. The file name is server.txt. The file is in the root directory of the CD or the directory where you unzipped or untarred the client package. After installing, the server README is located in /usr/ldap/web/*lang*/readme/server.txt or /usr/ldap/web/*lang*/readme/server.pdf, or at /usr/ldap/web/*lang*/readme/server.htm for viewing with a Web browser.

lang is the locale you chose when you installed IBM Directory Server.

In addition to the client requirements, the server requires the following:

- A minimum of 256 MB RAM (512 MB or more is strongly recommended).
- If you plan to use the InstallShield GUI to install, the Configuration Tool for configuration, or the embedded version of WebSphere® Application Server - Express, V5.0, see "AIX operating system client requirements" on page 5 for Java requirements.
- DB2 Universal Database for AIX version 8.1 Workgroup Server Edition (DB2) is included with the IBM Directory Server, although DB2 version 7.2 with FixPak 5 or higher is also supported.

  If you use DB2 version 8.1, the following versions of AIX are supported:

  – AIX version 4.3.3.0 with maintenance level 9 or later (32-bit)
  – AIX version 5L with maintenance level 2 or later (32-bit)

  In addition, the following AIX filesets are required to install or run DB2 in languages other than English:

– X11.fnt.ucs.ttf (AIX Windows Unicode True Type Fonts)
– XlC.rte 5.0.2.x

For Asian languages, the following filesets are also required:
– X11.fnt.ucs.ttf_CN (for zh_CN or Zh_CN)
– X11.fnt.ucs.ttf_KR (for ko_KR)
– X11.fnt.ucs.ttf_TW (for zh_TW or Zh_TW)

On AIX version 4.3.3 the following fileset is required: xIC.aix43.rte 5.0.2.x.

On AIX version 5L the following fileset is required: xIC.aix50.rte 5.0.2.x.

AIX filesets can be downloaded from
http://techsupport.services.ibm.com/server/fixes

Java Runtime Environment (JRE) version 1.3.1 is required to run DB2 servers and DB2 Java-based tools, such as the Control Center.

If you plan to use the Tivoli® Storage Manager facilities to back up and restore your databases, the Tivoli Storage Manager Client Version 4.2.0 is required.

A browser is required to view online help.

Attention: If you have SecureWay Directory Version 3.1.1.5, 3.2, 3.2.1, or 3.2.2, or IBM Directory Server 4.1 installed, read and understand the migration process in Chapter 3, "Migration from previous releases" on page 17 before removing or upgrading DB2. If you remove DB2 before migrating, you will lose your data.

Notes:

1. If you already have DB2 installed, you need approximately 30 MB of disk space to create the empty database and start the server. (DB2 requires about 300-500 MB of disk space.) IBM Directory Server (including the client and the server) requires about 160 MB.
2. Disk space required for data storage is dependent upon the number and size of database entries. Allow a minimum of 80 MB for your database on UNIX systems. Also, ensure that there is approximately another 4 MB of disk space in the /home directory to create the DB2 instance. See the README file for any last minute changes to database requirements.

You can choose to have more than one version of DB2 installed on a system. IBM Directory Server always uses, by default, the highest (newest) version of DB2 found on a system. If you want to use an older (supported) version of DB2, you must manually reset two links to enable that version, as shown in the following notes:

Notes:

1. If DB2 UDB 7.2 with FixPak 5 or later is installed, but not installed as the default database, issue the following commands as **root** to use it:

   ```
   ln -fs /usr/lpp/db2_07_01 /usr/ldap/db2
   ln -fs /usr/lpp/db2_07_01/lib/libdb2.a /usr/ldap/lib/libdb2.a
   ```

2. You must have a license to use any DB2 product other than DB2 UDB 8.1, which is delivered with IBM Directory Server.
3. If you are upgrading your level of DB2, ensure that you follow the DB2 migration procedure, which requires you to stop all applications. If you have a server up and running and you uninstall DB2 without reinstalling the IBM Directory Server, the directory server cannot start.

HP-UX operating system server requirements

Before installing, see the server README file for any updated information about supported versions of HP-UX. The file name is server.txt. The file is in the root directory of the CD or the directory where you unzipped or untarred the client package. After installing, the server README is located in /usr/IBMldap/web/*lang*/readme/server.txt or /usr/IBMldap/web/*lang*/readme/server.pdf, or at /usr/IBMldap/web/*lang*/readme/server.htm for viewing with a Web browser.

lang is the locale you chose when you installed IBM Directory Server.

In addition to the client requirements, the server requires the following:

- A minimum of 512 MB RAM .
- DB2 Universal Database for AIX version 8.1 Enterprise Server Edition (DB2) is included with the IBM Directory Server, although DB2 version 7.2 with FixPak 5 or higher is also supported.
- HP-UX Runtime Environment for the Java 2 Platform Version 1.3.1. HP-UX Runtime Environment for the Java 2 Platform Version 1.3.1. is included with IBM Directory Server.
- Current kernel configuration parameters. See "Setting the current kernel configuration parameters" on page 45 for the required parameters.

Notes:

1. If you already have DB2 installed, you need approximately 30 MB of disk space to create the empty database and start the server. (DB2 requires about 300-500 MB of disk space.) IBM Directory Server (including the client and the server) requires about 160 MB.
2. Disk space required for data storage is dependent upon the number and size of database entries. Allow a minimum of 80 MB for your database on UNIX systems. Also, ensure that there is approximately another 4 MB of disk space in the /home directory to create the DB2 instance. See the README file for any last minute changes to database requirements.

Linux or Linux for S/390 operating system server requirements

Before installing, see the server README file for any updated information about supported versions of Linux and Linux for S/390. The file name is server.txt. The file is in the root directory of the CD or the directory where you unzipped or untarred the client package. After installing, the server README file is located in /usr/ldap/web/*lang*/readme/server.txt or /usr/ldap/web/*lang*/readme/server.pdf, or at /usr/ldap/web/*lang*/readme/server.htm for viewing with a Web browser.

lang is the locale you chose when you installed IBM Directory Server.

In addition to the client requirements, the server requires the following:

- A minimum of 256 MB RAM (512 MB or more is strongly recommended).
- DB2 Universal Database for Linux version 8.1 Workgroup Server Edition (DB2) is included with the IBM Directory Server, although DB2 version 7.2 with FixPak 5 or higher is also supported.

Attention: If you have SecureWay Directory Version 3.1.1.5, 3.2, 3.2.1, or 3.2.2, or IBM Directory Server installed, read and understand the migration process in Chapter 3, "Migration from previous releases" on page 17 before removing or upgrading DB2. If you remove DB2 before migrating, you will lose your data.

Notes:

1. If you already have DB2 installed, you need approximately 30 MB of disk space to create the empty database and start the server. (DB2 requires about 300-500 MB of disk space.) IBM Directory Server (including the client and the server) requires about 160 MB.
2. Disk space required for data storage is dependent upon the number and size of database entries. Allow a minimum of 80 MB for your database on UNIX systems. Also allow approximately another 4 MB of disk space in the /home directory to create the DB2 instance. See the README file for any additional information about database requirements.

- On SuSE 7.0 and Red Hat 7.2 on Linux for S/390 with kernel level 2.4.x, you must download and install the compat-libstdc++-2.10.0-1.s390.rpm package. This package contains compatibility Standard C++ libraries that allow older binaries (created with old versions of compilers) to execute.

  Even after this change, the **ldapcfg**, **ldapucfg** and **ldapxcfg** programs fail on both SuSE 7.0 and Red Hat 7.2 systems. To correct the problem, edit the /usr/ldap/bin/ldapcfg script to uncomment the following line by removing the # in the first column of the line:

  ```
  export LD_PRELOAD=/usr/lib/libstdc++-libc6.2-2.so.3
  ```

  You must specify the absolute path of the library.
- If you plan to use the InstallShield GUI to install or the Configuration Tool for configuration on Linux, see "Linux operating system client requirements" on page 6 for Java requirements.

Solaris operating system server requirements

Before installing, see the server README file for any updated information about supported versions of Solaris. The file name is server.txt. The file is in the root directory of the CD or the directory where you unzipped or untarred the client package. After installing, the server README file is located in /opt/IBMldaps/web/*lang*/README/server.txt or /opt/IBMldaps/web/*lang*/README/server.pdf, or at /opt/IBMldaps/web/*lang*/README/server.htm for viewing with a Web browser.

lang is the locale you chose when you installed IBM Directory Server.

In addition to the client requirements, the server requires the following:

- A minimum of 256 MB RAM (512 MB is strongly recommended)
- On Solaris 7, the following patch levels are required to run the LDAP configuration programs (**ldapcfg**, **ldapxcfg**, **ldapucfg**):
  - 109104-01 (needed for 106541-12)
  - 107544-02 (needed for 106541-12)
  - 106541-12 (needed for 106980-13)
  - 106980-13
  - 107081-22
  - 107636-05
  - 108376-07 (needed for Asian locales only)

– 107544-03 109104-04 X11.adt.lib 4.3.3.0

Note: You can download Solaris operating system patches directory from Sun Microsystems, Inc. at the following Web site:

http://sunsolve.Sun.com

- If you plan to use the InstallShield GUI to install or the Configuration Tool for configuration, see "Solaris operating system client requirements" on page 7 for Java requirements.
- DB2 Universal Database for Solaris version 8.1 Workgroup Server Edition (DB2) is included with the IBM Directory Server, although DB2 version 7.2 with FixPak 5 or higher is also supported.

  If you use DB2 8.1, the following patches are required:

  – On Solaris 7 (32-bit): ″Recommended & Security Patches″ + 107226-17 + 107153-01 + 106327-10
  – On Solaris 7 (64-bit): ″Recommended & Security Patches″ + 107226-17 + 107153-01 + 106300-11
  – On Solaris 8 (32-bit): ″Recommended & Security Patches″ + 108921-12 + 108940-24 + 108434-03 and 108528-12
  – On Solaris 8 (64-bit): ″Recommended & Security Patches″ + 108921-12 + 108940-24 + 108435-03 and 108528-12

  ″Recommended & Security Patches″ can be obtained from the http://sunsolve.Sun.com Web site. On the SunSolve Online Web site, click on the**Patches** menu item in the left-hand panel and select **Recommended & Security Patches** from the **Browse & Download Patches** section.

  The J2SE Solaris Patch Clusters are also required. They can be obtained from the http://sunsolve.Sun.com Web site. From the SunSolve Online Web site, click on the **Patches** menu item in the left-hand panel and select **Recommended & Security Patches** from the **Browse & Download Patches** section.

  The SUNWlibC software is required to install DB2 on Solaris.

  You will need a Java Runtime Environment (JRE) Version 1.3.1 to run the DB2 Java-based tools, such as the Control Center, and to create and run Java applications, including stored procedures and user-defined functions. During the installation process, if the correct level of the JRE is not already installed, it will be installed.

  A browser is required to view online help.

  Attention: If you have SecureWay Directory Version 3.1.1.5, 3.2, 3.2.1, or 3.2.2, or IBM Directory Server 4.1 installed, read and understand the migration process in Chapter 3, "Migration from previous releases" on page 17 before removing or upgrading DB2. If you remove DB2 before migrating, you will lose your data.

  Notes:

  1. If you already have DB2 installed, you need approximately 30 MB of disk space to create the empty database and start the server. (DB2 requires about 300-500 MB of disk space.) IBM Directory Server (including the client and the server) requires about 160 MB.
  2. Disk space required for data storage is dependent upon the number and size of database entries. You need to allow a minimum of 80 MB for your

database on UNIX systems. Also allow another 2 to 3 MB of disk space to create the DB2 instance. See the README file for any last minute changes on database requirements.

- Current kernel configuration parameters. See "Setting the current kernel configuration parameters" on page 45 for the required parameters.

Windows 2000 or Windows NT operating systems server requirements

Before installing, see the server README file for any updated information about supported versions of the Windows 2000 or Windows NT operating system. The README file is in the root directory of the CD or the directory where you unzipped or untarred the client package. After installing, the README file is located in *installpath*\web*lang*\readme\server.txt or *installpath*\web*lang*\readme\server.pdf, or at *installpath*\web*lang*\readme\server.htm for viewing with a Web browser.

installpath is the location where the IBM Directory Server client is installed.

lang is the locale you chose when you installed IBM Directory Server. For example, for United States English the locale is en_US.

In addition to the client requirements, the server requires the following:

- Windows 2000, or Windows NT 4.0 with Service Pack 6 or later. (The server is not supported on Windows XP.)
- A minimum of 256 MB RAM (512 MB is strongly recommended.)
- The minimum supported level of DB2 is DB2 Version 7.2 with FixPak 5 or later. DB2 Version 8.1 Workgroup Server Edition is included with the IBM Directory Server and is installed, if a supported version of DB2 is not detected on your system. If you have a version of DB2 earlier than Version 7.2 with FixPak 5 installed on your system, you must remove it or upgrade it before installing the IBM Directory version 5.1.

  Attention: If you have SecureWay Directory Version 3.1.1.5, 3.2, 3.2.1, or 3.2.2 installed, read and understand the migration process in Chapter 3, "Migration from previous releases" on page 17 before removing or upgrading DB2. If you remove DB2 before migrating, you will lose your data.

  Notes:

  1. If you already have DB2 installed, you need approximately 25 MB of disk space to create the empty database and start the server. (DB2 requires about 300-500 MB of disk space.) IBM Directory Server (including the client and the server) requires about 110 MB.
  2. Disk space required for data storage is dependent upon the number and size of database entries. Allow a minimum of 80 MB for your database on Windows 2000 or Windows NT systems. Also allow another 2 to 3 MB of disk space when creating the DB2 instance. See the README file for any last minute changes to database requirements.

Requirements for the Web Administration Tool

The Web Administration Tool is supported on all operating system platforms supported for the client or the server. You can install the Web Administration Tool on a computer with or without the client or the server. To use the Web Administration Tool to administer servers, you need the following:

- One of the following application servers:

– embedded version of WebSphere Application Server - Express, V5.0 (Provided with IBM Directory Server)

Note: The embedded version of WebSphere Application Server - Express, V5.0 is not available for HP-UX. If you want to use the Web Administration Tool on HP-UX, you must download and install Apache Tomcat 4.0.3.

– Apache Tomcat 4.0.3 plus one of the following versions of Java:
  - IBM version 1.3.1, Service release 2 (and up for 1.3.1, but not 1.4)
  - Sun version 1.3.1_4
  - HP-UX version 1.3.1.06

- One of the following Web browsers on the computer from which you will use the Web Administration Tool. (This might or might not be the computer where the Web Administration Tool is installed):

  On AIX
  – Netscape version 7.0

  On HP-UX 11i
  – Netscape version 6.2.3 or 7.0
  – Microsoft Internet Explorer version 5.0

  On Linux
  – On all Linux distributions: Netscape version 6.2.3 or 7.0

  On Solaris 7, 8, or 9
  – Netscape version 6.2.3 or 7.0
  – Microsoft Internet Explorer version 5.0

  On Windows NT, 2000, and XP
  – Microsoft Internet Explorer version 5.5
  – Netscape version 6.2.3 or 7.0

Secure Sockets Layer (SSL) Global Security Kit (GSKit)

Global Security Kit (GSKit) version 6.0.3 is an optional software package that is required only if Secure Sockets Layer (SSL) Security is required.

The IBM Directory Server 5.1 alone does not provide the capability for SSL connections from IBM Directory Server clients. You can enable the SSL feature by installing the IBM GSKit 6.0.3 package. The GSKit package includes SSL support and associated RSA Data Security, Inc. (4) technology.

The IBM Directory Server server can work without the GSKit installed. In this case the IBM Directory Server server accepts only non-SSL connections from any Directory client. Similarly, the IBM Directory Server client can work without the GSKit installed. Install GSKit on both the server and the client if you want to use SSL connections.

See Appendix G, “Setting up GSKit to support CMS key databases” on page 105 for more information about setting up GSKit after installation.

Chapter 3. Migration from previous releases

Migrating is necessary to preserve any changes that you have made to the schema definitions and to preserve your data and directory server configuration. Use the procedures in this chapter when you are migrating an existing directory server on the same physical computer from a version of SecureWay Directory or from IBM Directory Server 4.1.

If your installation includes replica servers, see Appendix C, "Migrating a network of replicating servers" on page 93 for additional information before you start migrating any of your servers.

Note: If you have only a client installed, migration is generally not necessary. However, if you are migrating from a release prior to IBM Directory Server 4.1 and you have Java applications that use the IBM JNDI jar files, the jar files will be removed during installation; therefore, save them before you install IBM Directory Server 5.1. See step 3 on page 19 for Windows platforms or step 3 on page 23 for all UNIX platforms for information.

Starting with IBM Directory Server 4.1, IBM JNDI is not supported. IBM Directory Server 4.1 and IBM Directory Server 5.1 include the Sun Microsystems JNDI. See the Sun documentation for information about the Sun JNDI. There might be some functional differences between IBM and Sun implementations that require changes to existing JNDI applications. IBM JNDI applications might still run, but it is recommended that you begin using the Sun JNDI immediately.

Use one of the following sections to migrate a directory server, depending on what version you are migrating from and the operating system you are using:

If you are migrating from SecureWay Directory, see one of the following sections:

- For Windows, see "Migration from SecureWay Directory Version 3.2.x for Windows InstallShield GUI installations" on page 18.
- For AIX, see "Migration from SecureWay Directory Version 3.2.x for AIX installations" on page 20.
- For Solaris, Linux, Linux for S/390, or HP-UX, see "Migration from SecureWay Directory Version 3.2.x for UNIX installations" on page 22.

Note: In releases before IBM Directory Server 4.1, the LDAP server uses **LDAP** as its Kerberos service name to communicate with its client and the Kerberos KDC. (For example, LDAP/ldaphost.austin.ibm.com, where ldaphost is the hostname of the computer where the LDAP server is located.) For IBM Directory Server 4.1 and 5.1, a lowercase service name is used (for example, ldap/ldapname.austin.ibm.com). Because of this change, an IBM Directory Server 4.1 or 5.1 server might not be able to start after migrating from a 3.x server. This is because the 4.1 or 5.1 server is looking for **ldap** in the keytab file in which an **LDAP** service name was located and used by the previous 3.x server. To correct this situation you can do either of the following:

- Generate a keytab file by adding a lowercase LDAP Kerberos service name and start using the new keytab file to communicate.
- Set the environment variable LDAP_KRB_SERVICE_NAME to **LDAP** before starting the server. This environment variable causes the LDAP

server to continue using the uppercase LDAP server service name in the keytab file and to communicate with its clients. In the latter case, the environment variable must be set on the client side as well so that the client will continue using the uppercase LDAP service name to communicate with its server.

If you are migrating from IBM Directory Server 4.1, see one of the following sections:

- For Windows, see "Migration from IBM Directory Server version 4.1 for Windows installations" on page 25.
- For AIX, see "Migration from IBM Directory Server version 4.1 for AIX installations" on page 25.
- For Solaris, Linux, Linux for S/390, or HP-UX, see "Migration from IBM Directory Server Version 4.1 for UNIX installations" on page 25.

The version of SecureWay Directory you are migrating must be 3.2.0 or higher. If you have SecureWay Directory 3.1.1.5 version currently installed, you must upgrade to version 3.2.2 before installing IBM Directory Server 5.1. You can download SecureWay Directory version 3.2.2 from the IBM SecureWay Directory Web site: http://www-4.ibm.com/software/network/directory/downloads/.

The audit log and the change log are not migrated. If you want to preserve your audit log and change log settings, record them before proceeding. After you have installed IBM Directory Server, you can reset the audit log settings through the Web Administration Tool and the change log settings through the Configuration Tool.

Attention: Run the **db2ldif** application before uninstalling the 3.2.x version of SecureWay Directory. Do not use the **DB2BACKUP** command.

Reference your current (pre-IBM Directory Server 5.1) documentation for instructions and recommendations for running the **db2ldif** utility. Databases must not be unconfigured or dropped unless they have been backed up using the 3.2.x or 4.1 version of **db2ldif**. Failure to comply with this results in a complete loss of data.

Migration from SecureWay Directory Version 3.2.x for Windows InstallShield GUI installations

If you are upgrading from a 3.2.x version of SecureWay Directory, and you are installing IBM Directory Server on a Windows 2000 or Windows NT system using the InstallShield GUI, the installation automatically completes some migration for you.

To migrate, do the following:
Pre-installation steps:

1. Back up the previous versions of the slapd32.conf and any schema files from the *install path*\etc directory to the *install path*\etc\userV51 directory. (You must create the *install path*\etc\userV51 directory.) *install path* is the directory where SecureWay Directory is installed.

   These files have the following file extensions:

   - .oc
   - .at

- .conf

2. Back up the following files:
   - V3.ldapsyntaxes
   - V3.matchingrules
   - V3.modifiedschema
3. If you have any existing IBM JNDI applications, IBMJNDI.JAR or any associated JNDI files, you can save them if you like, although IBM JNDI is no longer supported. To save the files:
   - Save files, including any subdirectories, in *install path*\jre\bin to *install path*\etc\userV51\jre\bin
   - Save files, including any subdirectories, in *install path*\jre\lib to *install path*\etc\userV51\jre\lib

   JNDI-related files are:
   - Ibmjcefw.jar
   - Ibmjceprovider.jar
   - IBMjgssprovider.jar
   - Local_policy.jar
   - US_export_policy.jar
   - Krb5.ini
   - Ibmjndi.jar
   - Ibmjndi.zip
4. If you have not done so already:
   a. Export the database using **db2ldif**:

      ```
      db2ldif -o outputfile
      ```

      where *outputfile* specifies the LDIF output file to contain the directory entries in LDIF format.

      For more information about the **db2ldif** command, read the **db2ldif** documentation in the *SecureWay Administration Guide* for your release before exporting the database.

      Attention: Do not use the **DB2BACKUP** command to export your data. If you do not export using **db2ldif** before unconfiguring and removing the database, you will lose your data.

   b. Unconfigure and remove the database by typing the following at a command prompt:

      ```
      ldapucfg -d
      ```

      Type **y** to confirm the removal. Default LDAP databases are automatically removed from the system when the command successfully completes.

      Notes:

      1) If you use a custom database, you must manually remove the DB2 database from the system.
      2) Data contained in the SecureWay Directory 3.2.x database is not compatible with IBM Directory Server 5.1 unless it is exported via **db2ldif** and imported through the **bulkload** utility provided with IBM Directory Server 5.1.
      3) The server will not start if you do not migrate the database.

4) The changes in the changelog database are not compatible with the new data format and cannot be used. The existing changelog settings contained in the slapd32.conf file will be migrated to the new configuration.
5) The audit log will not be migrated and must be reconfigured.
6) If you have a downlevel version of DB2, you must upgrade to DB2 7.2 FixPak 5 or later after you have exported the database. Alternatively, you can remove DB2 after you have exported the database and install the version of DB2 provided with IBM Directory Server.

Installation steps:

5. Install IBM Directory Server 5.1 using the InstallShield GUI. See "Installing IBM Directory Server 5.1 on a Windows platform" on page 28 for instructions. The InstallShield GUI automatically migrates the configuration and schema files.

   Notes:

   a. You might be asked if you want to replace some configuration files. Select **Yes** to replace.
   b. If a configured database is detected, you are instructed that additional steps must be taken before the installation can continue. The installation program lists the steps needed to be taken before the installation can continue. The installation program exits after you acknowledge that these steps are required. The IBM Directory Server installation program repeats this behavior as long as there is an existing database configured.

Post-installation steps:

6. After you complete installation and restart your computer, the Configuration Tool starts automatically. Use the Configuration Tool to set the Administrator DN and password and configure a new LDAP database. See Chapter 10, "Configuration" on page 63 for instructions on how to configure the LDAP database.

   Note: If you want a change log database, make sure change log is enabled through the Configuration Tool or by using the **ldapcfg** utility with the **-g** option.

7. Use the **bulkload** utility to import the **db2ldif** exported data, as follows:

   ```
   bulkload -i ldiffile -c -d
   ```

   where *ldiffile* is the name of the input file containing the LDIF data to be loaded into the directory.

   Note: Read the **bulkload** documentation in the *IBM Directory Server Version 5.1 Administration Guide* for information about new command line settings that provide additional levels of function.

Migration from SecureWay Directory Version 3.2.x for AIX installations

The instructions in this section are for AIX installations. For Solaris, Linux, and Linux for S/390, see "Migration from SecureWay Directory Version 3.2.x for UNIX installations" on page 22.

To migrate an existing directory server on AIX:
Pre-installation steps:

1. Back up the previous versions of the slapd32.conf and any schema files from the *install path*/etc directory to the *install path*/etc/userV51 directory. (You must create the *install path*/etc/userV51 directory.) *install path* is the directory where SecureWay Directory is installed.

   These files have the following file extensions:

   - .oc
   - .at
   - .conf

2. Back up the following files:
   - V3.ldapsyntaxes
   - V3.matchingrules
   - V3.modifiedschema
3. If you have any existing IBM JNDI applications, IBMJNDI.JAR or any associated JNDI files, you can save them if you like, although IBM JNDI is no longer supported. To save the files:
   - Save files, including any subdirectories, in *install path*\java\bin to *install path*\etc\userV51\java\bin
   - Save files, including any subdirectories, in *install path*\java\lib to *install path*\etc\userV51\java\lib

   JNDI-related files are:
   - Ibmjcefw.jar
   - Ibmjceprovider.jar
   - IBMjgssprovider.jar
   - Local_policy.jar
   - US_export_policy.jar
   - Krb5.ini
   - Ibmjndi.jar
   - Ibmjndi.zip
4. Export the database using **db2ldif**, as follows:

   ```
   db2ldif -o outputfile
   ```

   where *outputfile* specifies the LDIF output file to contain the directory entries in LDIF format.

   For more information about the **db2ldif** command, read the **db2ldif** documentation in the *SecureWay Administration Guide* for your release before exporting the database.

   Attention: Do not use the **DB2BACKUP** command to export your data. If you do not export using **db2ldif** before unconfiguring and removing the database, you will lose your data.
5. Unconfigure and remove the database by typing the following at a command prompt:

   ```
   ldapucfg -d
   ```

   Type **y** to confirm the removal. Default LDAP databases are automatically removed from the system when the command successfully completes.

Notes:

a. If you use a custom database, you must manually remove the DB2 database from the system.

b. Data contained in the SecureWay Directory 3.2.x database is not compatible with IBM Directory Server 5.1 unless it is exported via **db2ldif** and imported through the **bulkload** utility provided with IBM Directory Server 5.1.

c. The server will not start if you do not migrate the database.

d. If you have a downlevel version of DB2, you must upgrade to DB2 7.2 FixPak 5 or later after you have exported the database. Alternatively, you can remove DB2 after you have exported the database and install the version of DB2 provided with IBM Directory Server.

e. The changes in the change log database are not compatible with the new data format and cannot be used. The existing change log settings contained in the slapd32.conf file will be migrated to the new configuration.

f. The audit log will not be migrated and must be reconfigured.

Installation steps:

6. Install IBM Directory Server 5.1 using SMIT. For information, see "SMIT installation" on page 39.

Post-installation steps:

7. Migrate the configuration and schema by executing the migrate51 script. Type the following at a command prompt:

   ```
   cd installpath/etc
   ../sbin/migrate51
   ```

   Note: You must run the migrate51 script even if you did not modify the previous schema. There are new schema files and entries in the ibmslapd.conf file that are not compatible with previous versions.

8. Set the Administrator DN and password and configure a new LDAP database using the **ldapcfg** or **ldapxcfg** commands. See Chapter 10, "Configuration" on page 63 for instructions on how to configure the LDAP database.

   Note: If you want a change log database, make sure change log is enabled through the Configuration Tool or by using the **ldapcfg** command with the **-d** option.

9. Use the **bulkload** utility to import the **db2ldif** exported data:

   ```
   bulkload -i ldiffile -c -d
   ```

   where *ldiffile* is the name of the input file containing the LDIF data to be loaded into the directory.

   Note: Read the **bulkload** documentation in the *IBM Directory Server Version 5.1 Administration Guide* for new command line settings that provide additional levels of function.

Migration from SecureWay Directory Version 3.2.x for UNIX installations

The instructions in this section are for Solaris, Linux, and Linux for S/390. Do not use these instructions to migrate on an AIX system. If you are migrating on an AIX system, see "Migration from SecureWay Directory Version 3.2.x for AIX installations" on page 20.

To migrate an existing directory server:

Pre-installation steps:

1. Back up the previous versions of the slapd32.conf and any schema files from the *install path*/etc directory to the *install path*/etc/userV51 directory. (You must create the *install path*/etc/userV51 directory.) *install path* is the directory where SecureWay Directory is installed.

   These files have the following file extensions:

   - .oc
   - .at
   - .conf

2. Back up the following files:
   - V3.ldapsyntaxes
   - V3.matchingrules
   - V3.modifiedschema
3. If you have any existing IBM JNDI applications, IBMJNDI.JAR or any associated JNDI files, you can save them if you like, although IBM JNDI is no longer supported. To save the files:
   - Save files, including any subdirectories, in *install path*\java\bin to *install path*\etc\userV51\java\bin
   - Save files, including any subdirectories, in *install path*\java\lib to *install path*\etc\userV51\java\lib

   JNDI-related files are:
   - Ibmjcefw.jar
   - Ibmjceprovider.jar
   - IBMjgssprovider.jar
   - Local_policy.jar
   - US_export_policy.jar
   - Krb5.ini
   - Ibmjndi.jar
   - Ibmjndi.zip
4. Export the database using **db2ldif**, as follows:

   Note: Read the **db2ldif** documentation in the *SecureWay Administration Guide* for your release before exporting the database.

   ```
   db2ldif -o outputfile
   ```

   where *outputfile* specifies the LDIF output file to contain the directory entries in LDIF format.

Attention: Do not use the **DB2BACKUP** command to export your data. If you do not export using **db2ldif** before unconfiguring and removing the database, you will lose your data.

5. Unconfigure and remove the database by typing the following at a command prompt:

   ```
   ldapucfg -d
   ```

   Type **y** to confirm the removal. Default LDAP databases are automatically removed from the system when the command successfully completes.

Notes:

a. If you use a custom database, you must manually remove the DB2 database from the system.

b. Data contained in the SecureWay Directory 3.2.x database is not compatible with IBM Directory Server 5.1 unless it is exported via **db2ldif** and imported through the **bulkload** utility provided with IBM Directory Server 5.1.

c. The server will not start if you do not migrate the database.

d. If you have a downlevel version of DB2, you must upgrade to DB2 7.2 FixPak 5 or later after you have exported the database. Alternatively, you can remove DB2 after you have exported the database and install the version of DB2 provided with IBM Directory Server.

e. The changes in the changelog database are not compatible with the new data format and cannot be used. The existing changelog settings contained in the slapd32.conf file will be migrated to the new configuration.

f. The audit log will not be migrated and must be reconfigured.

6. Uninstall SecureWay Directory 3.2.x.

Installation steps:

7. Install IBM Directory Server 5.1. Use one of the following:
   - **pkgadd** for Solaris. See "Command line installation using pkgadd" on page 56 for information.
   - **RPM** for Linux (Intel) and Linux for S/390. See "Installing the IBM Directory Server" on page 49 for information.

Post-installation steps:

8. Migrate the configuration and schema by executing the migrate51 script. Type the following at a command prompt:

   ```
   cd installpath/etc
   ../sbin/migrate51
   ```

   Note: You must run the migrate51 script even if you did not modify the previous schema. There are new schema files and entries in the ibmslapd.conf file that are not compatible with previous versions.

9. Set the Administrator DN and password and configure a new LDAP database using the **ldapcfg** or **ldapxcfg** commands. See Chapter 10, "Configuration" on page 63 for instructions on how to configure the LDAP database.

   Note: If you want a change log database, make sure change log is enabled through the Configuration Tool or the **ldapcfg** command with the **-d** option.

10. Use the **bulkload** utility to import the **db2ldif** exported data:

    ```
    bulkload -i ldiffile -c -d
    ```

    where *ldiffile* is the name of the input file containing the LDIF data to be loaded into the directory.

    Note: Read the **bulkload** documentation in the *IBM Directory Server Version 5.1 Administration Guide* for new command line settings that provide additional levels of function.

Migration from IBM Directory Server version 4.1 for Windows installations

If you are upgrading from the 4.1 version of IBM Directory Server on a Windows 2000 or Windows NT system using the InstallShield GUI, migration is automated. The InstallShield GUI backs up the slapd32.conf and schema files before installing the 5.1 version, and it migrates these files to the 5.1 version for you automatically.

Migration from IBM Directory Server version 4.1 for AIX installations

The instructions in this section are for AIX installations. For Solaris, Linux, Linux for S/390, and HP-UX, see "Migration from IBM Directory Server Version 4.1 for UNIX installations".

To migrate an existing directory server on AIX:
Pre-installation steps:

1. Back up the previous versions of the slapd32.conf and any schema files from the *install path*/etc directory to the usr/ldap/etc/userV51 directory. (You must create the usr/ldap/etc/userV51 directory.)

   These files have the following file extensions:

   - .oc
   - .at
   - .conf
2. Back up the following files:
   - V3.ldapsyntaxes
   - V3.matchingrules
   - V3.modifiedschema

Installation steps:

3. Install IBM Directory Server 5.1 using SMIT. See "SMIT installation" on page 39 for information.

Post-installation steps:

4. Migrate the configuration and schema by executing the migrate51 script. Type the following at a command prompt:

   ```
   cd installpath/etc
   ../sbin/migrate51
   ```

   Note: You must run the migrate51 script even if you did not modify the previous schema. There are new schema files and entries in the ibmslapd.conf file that are not compatible with previous versions.

Migration from IBM Directory Server Version 4.1 for UNIX installations

The instructions in this section are for Solaris, Linux, Linux for S/390, and HP-UX. Do not use these instructions to migrate on an AIX system. If you are migrating on an AIX system, see "Migration from IBM Directory Server version 4.1 for AIX installations".

To migrate an existing directory server:
Pre-installation steps:

1. Back up the previous versions of the slapd32.conf and any schema files from the *install path*/etc directory to the *install path*/etc/userV51 directory. (You must create the *install path*/etc/userV51 directory.) *install path* is the directory where IBM Directory Server 4.1 is installed.

   These files have the following file extensions:

   - .oc
   - .at
   - .conf

2. Back up the following files:
   - V3.ldapsyntaxes
   - V3.matchingrules
   - V3.modifiedschema
3. Uninstall IBM Directory Server 4.1. (Do **not** uninstall on HP-UX.)

Installation steps:

4. Install IBM Directory Server 5.1 using one of the following:
   - **pkgadd** for Solaris. See "Command line installation using pkgadd" on page 56 for information.
   - **RPM** for Linux (Intel) and Linux for S/390. See "Installing the IBM Directory Server" on page 49 for information.
   - **swinstall** for HP-UX. See Chapter 6, "Installing using HP-UX utilities" on page 45 for information.
5. Migrate the configuration and schema by executing the migrate51 script. Type the following at a command prompt:

   ```
   cd installpath/etc
   ../sbin/migrate51
   ```

   Note: You must run the migrate51 script even if you did not modify the previous schema. There are new schema files and entries in the ibmslapd.conf file that are not compatible with previous versions.

Chapter 4. Installing with the InstallShield GUI

You can use the InstallShield GUI to install IBM Directory Server on AIX, Solaris, Windows 2000, Windows NT, or Windows XP platforms. It is also available for Linux SuSE and Linux Red Hat platforms. If you do not want to use the InstallShield GUI to install, this guide contains a manual installation chapter for each platform. For an example, see Chapter 5, "Installing using AIX utilities" on page 39.

The InstallShield GUI requires a substantial amount of temporary disk space. Before installing, ensure that you have at least 400® MB of available space in your /tmp directory on UNIX platforms, or at least 100 MB of available space in the directory specified by the TEMP environment variable on Windows platforms.

Attention: You cannot migrate from a version of SecureWay Directory or from the 4.1 version of IBM Directory Server, or reinstall over an existing version of IBM Directory Server 5.1 on a UNIX platform using the InstallShield GUI. Use the operating system utilities for your operating system to install IBM Directory Server if you want to migrate or reinstall.

See "Migration from SecureWay Directory Version 3.2.x for AIX installations" on page 20 or "Migration from IBM Directory Server version 4.1 for AIX installations" on page 25 for instructions on migrating and restoring backed-up files after reinstallation on an AIX system.

Read and understand the migration process in "Migration from SecureWay Directory Version 3.2.x for UNIX installations" on page 22 or "Migration from IBM Directory Server Version 4.1 for UNIX installations" on page 25 for instructions for migrating and restoring backed-up files after reinstallation on a Linux, Solaris, or HP-UX system.

If you have SecureWay Directory version 3.1.1.5, 3.2, 3.2.1, or 3.2.2 or IBM Directory Server 4.1 installed on a Windows 2000 or Windows NT system, read and understand the migration process in "Migration from SecureWay Directory Version 3.2.x for Windows InstallShield GUI installations" on page 18 or "Migration from IBM Directory Server version 4.1 for Windows installations" on page 25 before installing IBM Directory Server 5.1.

It is very important that you back up and export previous versions of schema files and the slapd32.conf file before installing IBM Directory Server 5.1.

Note: If you install using the InstallShield GUI, you must also uninstall using the InstallShield GUI. See "Uninstalling IBM Directory Server" on page 77 for instructions for removing IBM Directory Server using the InstallShield GUI.

Before installing on a Windows operating system using the InstallShield GUI

Before installing, make sure the following conditions are met. If these conditions are not met, the installation program will exit.

- **If you have a pre-3.2.x version of SecureWay Directory installed on your system:**

Upgrade to 3.2 or later before installing IBM Directory Server 5.1. Then use the instructions in Chapter 3, "Migration from previous releases" on page 17 to migrate your data and install IBM Directory Server 5.1.

- **If you have a downlevel version of DB2:**

  Upgrade to DB2 7.2 FixPak 5 or later, or remove DB2. DB2 8.1 is included with IBM Directory Server. If you do not have a version of DB2 on your system, the InstallShield GUI installs it.

  Attention: Export your data using **db2ldif** before unconfiguring and removing your current database. Do not use the **DB2BACKUP** command. If you do not export before unconfiguring and removing the database, you will lose your data.
- **If you have a 3.2.x version of SecureWay Directory installed on your computer**:

  Use the instructions in Chapter 3, "Migration from previous releases" on page 17 to migrate your data and install IBM Directory Server 5.1.
- **If you have a IBM Directory Server 4.1 installed on your computer**:

  Use the instructions in Chapter 3, "Migration from previous releases" on page 17 to migrate your data and install IBM Directory Server 5.1.

Creating the DB2 database owner

Before you install, create or be sure that you have created the user ID that will own the DB2 database used to store the directory data. You will be asked to provide this user ID during configuration, which runs automatically after installation and system restart. The user ID must be 8 characters or less, and it must be a member of the Administrators group. If you are creating a new database, a DB2 instance with the same name as the user ID will be created to hold the database.

Installing IBM Directory Server 5.1 on a Windows platform

The InstallShield GUI has two installation options: Typical and Custom. If you want to accept the default settings, select **Typical** during installation. If you are an experienced user and want to customize your installation, select **Custom**.

Note: After installation using the InstallShield GUI has begun, do not try to cancel the installation by closing the InstallShield window or using the **Ctrl+C** keystroke. If you inadvertently cancel installation, see "Recovering from a failed installation" on page 82 before you attempt to reinstall.

Typical installation for a Windows operating system

Typical installation uses default settings and is recommended for new users.

To install the IBM Directory Server 5.1:

1. On the computer where you are installing the IBM Directory Server, stop any programs that are running and close all windows. If you have open windows, the initial IBM Directory Server installation window might be hidden behind other windows.
2. If you are installing from a CD, insert the CD in your CD-ROM drive.

   If the CD-ROM does not automatically start the installation program, click **Start->Run**.

3. Depending on whether you are installing locally from a CD or remotely from the network, select the drive for your CD-ROM or for the appropriate network path. If you downloaded a zip or tar file, go to the directory where you unzipped or untarred the file.
4. In the \ismp folder, double-click the **setup.exe** icon.

   The language window is displayed.

   Note: When installing on Windows, if the installation program exits without displaying the language window, it might be caused by one of the following:
   - Backlevel video drivers. Update your video drivers to correct this.
   - Not enough space in the directory specified by the TEMP environment variable. Be sure that you have at least 100 MB of free space in this directory.
5. Select the language you want to use during IBM Directory Server installation. Click **OK**.

   Note: This is the language used in the installation program, not in the IBM Directory Server. You choose the language used in the IBM Directory Server in step 11 on page 30.
6. On the Welcome window, click **Next**.
7. If a previous or current version of IBM Directory Server is not installed on your system, go to step 8. If a previous or current version of IBM Directory Server is installed on your system, do one of the following:
   - **If you have a previous version of IBM Directory Server installed on your system:** You are asked if you want to migrate your configuration. Click **Yes** to migrate or **No** to overwrite your previous installation. If you click **Yes**, some migration processes will take place automatically during installation. See "Migration from SecureWay Directory Version 3.2.x for Windows InstallShield GUI installations" on page 18 for complete migration instructions.

     Attention: If you choose to click **No** and overwrite your previous installation, you will lose your data.
   - **If you have a previous version of the IBM Directory Client SDK installed on your system:** You are asked if you want to continue with the installation. Click **Yes** to install over the previous version of IBM Directory Client SDK, or click **No** to exit the installation program.
   - **If you have a current version of the IBM Directory Server, the IBM Directory Client SDK, or both installed on your system:** You will be asked if you want to exit the installation. If you do not exit and back up your files, they will be overwritten during the installation.
8. After reading the Software license agreement, click **I accept the terms in the license agreement**.
9. Click **Next**. Any preinstalled components and corresponding version levels are displayed. Click **Next**.
10. To install to the default directory, click **Next**. You can specify a different directory by clicking **Browse**.

    Note: Do not use special characters, such as hyphen (-) and period (.) in the name of the installation directory. If you do not use the default location, use a name such as **ldap** or **ldapdir**. Do not use a name such as **ldap-dir** or **ldap.dir**.

11. Select the language you want to use in IBM Directory Server 5.1. Click **Next**.
12. Click **Typical** and click **Next**.
13. The following list is displayed:
    - Client SDK 5.1
    - Web Administration 5.1
    - Server 5.1

    Notes:

    a. If you have an earlier version of a component installed on your computer, you must install the most current version of the component.

    b. If you select **Web Administration 5.1** and the embedded version of WebSphere Application Server - Express, V5.0 is not installed, it is installed for you.

    c. If you select **Web Administration 5.1**, DSML is also installed. See Appendix E, "Installing and configuring DSML" on page 99 for information about configuring DSML.

    Be sure the components you want to install are selected, and click **Next**.
14. If you selected **Server 5.1** in step 13, and DB2 is not installed on your system, DB2 8.1 will be installed for you. You will see a window prompting you to enter a Windows user ID and password for the DB2 system ID. The user ID default is **db2admin**. Type the user ID or accept the default.
15. Type the password, and then type the password again for verification.
    - If you are using an existing Windows user ID, be sure your password is correct. Otherwise, DB2 does not install correctly.
    - If you do not want to use an existing user ID, DB2 creates the user ID you specify with the password you type.
16. Click **Next**.
17. A window summarizing the components selected for installation and configuration is displayed.

    Note: Any corequisite products needed by the IBM Directory Server, such as DB2, are automatically installed. These products are listed in the summary described in this step.

    If you want to change any of your selections, click **Back**. To begin installation, click **Next**.
18. After the files are installed, the Client README file opens. Read the file and click **Next**. If you installed the server, the server README file also opens. Read the file and click **Next**.
19. Select to restart your computer now or later and click **Finish**.

    Attention: Before you restart the computer, be sure that you have created the user ID that will own the DB2 database. See "Creating the DB2 database owner" on page 28 for information about this user ID.

    If you installed the server, you must restart your system to complete the IBM Directory Server configuration. You are unable to use the IBM Directory Server product until this is completed. After the restart, the configuration program runs. The configuration program must complete before you can use the IBM Directory Server. See Chapter 10, "Configuration" on page 63 for more information about using the Configuration Tool to make changes to your configuration at a later time.

You have completed a Typical installation. To see a list of the installed components, click **Start->Programs->IBM Directory Server 5.1**.

After your computer is restarted, if you installed the server, the Configuration Tool automatically runs so that you can complete server configuration. Before you can use the server, you must set the administrator DN and password and configure the database that will store the directory data. To complete configuration, use the following instructions:

1. To set the administrator DN and password, use the instructions in "Setting the Administrator DN and password" on page 64.
2. To configure the database, use the instructions in "Configuring the database" on page 66.

You have completed server configuration.

To make changes to your configuration at a later time, see Chapter 10, "Configuration" on page 63 for more information about using the Configuration Tool.

Custom installation for a Windows operating system

Custom installation is for experienced users who want to customize their installations.

To install IBM Directory Server 5.1:

1. On the computer where you are installing the IBM Directory Server, stop any programs that are running and close all windows. If you have open windows, the initial IBM Directory Server installation window might be hidden behind other windows.
2. If you are installing from a CD, insert the CD in your CD-ROM drive.

   If the CD-ROM does not automatically start the installation program, click **Start->Run**.
3. Depending on whether you are installing locally from a CD or remotely from the network, select the drive for your CD-ROM or for the appropriate network path. If you downloaded a zip or tar file, go to the directory where you unzipped or untarred the file.
4. In the \ismp folder, double-click the **setup.exe** icon.

   The language window is displayed.

   Note: When installing on Windows, if the installation program exits without displaying the language window, it might be caused by one of the following:
   - Backlevel video drivers. Update your video drivers to correct this.
   - Not enough space in the directory specified by the TEMP environment variable. Be sure that you have at least 100 MB of free space in this directory.
5. Select the language you want to use during IBM Directory Server installation. Click **OK**.

   Note: This is the language used in the installation program, not in the IBM Directory Server. You choose the language used in the IBM Directory Server in step 11 on page 32.
6. On the Welcome window, click **Next**.

7. If a previous or current version of IBM Directory Server is not installed on your system, go to step 8. If a previous version of IBM Directory Server is installed on your system, do one of the following:
   - **If you have a previous version of the IBM Directory Server server installed on your system:** You are asked if you want to migrate your configuration. Click **Yes** to migrate or **No** to overwrite your previous installation. If you click **Yes**, some migration processes will take place automatically during installation. See "Migration from SecureWay Directory Version 3.2.x for Windows InstallShield GUI installations" on page 18 for complete migration instructions.

     Attention: If you choose to click **No** and overwrite your previous installation, you will lose your data.
   - **If you have a previous version of the IBM Directory Server Client SDK installed on your system:** You are asked if you want to continue with the installation. Click **Yes** to install over the previous version of IBM Directory Server Client SDK, or click **No** to exit the installation.
   - **If you have the current version of the IBM Directory Server server, the IBM Directory Server Client SDK, or both, installed on your system:** You will be asked if you want to exit the installation. If you do not exit and back up your files, they will be overwritten during the installation.
8. After reading the Software license agreement, select **I accept the terms in the license agreement**. Click **Next**.
9. Any preinstalled components and corresponding version levels are displayed. Click **Next**.
10. To install to the default directory, click **Next**. You can specify a different directory by clicking **Browse**.

    Note: Do not use special characters, such as hyphen (-) and period (.) in the name of the installation directory. If you do not use the default location, use a name such as **ldap** or **ldapdir**. Do not use a name such as **ldap-dir** or **ldap.dir**.
11. Select the language you want to use in IBM Directory Server 5.1. Click **Next**.
12. Click **Custom** and click **Next**.
13. A window showing the following components for installation is displayed:
    - Client SDK 5.1
    - Web Administration 5.1
    - Server 5.1
    - IBM WebSphere Application Server - Express
    - DB2 8.1
    - GSKit 6 (SSL packages only.)

    The components that are not yet installed are preselected. You can choose to reinstall the server or the client, if they were previously installed.

    Notes:

    a. If you select **Web Administration 5.1**, DSML is also installed. See Appendix E, "Installing and configuring DSML" on page 99 for information about configuring DSML.

    b. If you install the Web Administration Tool, an application server is required to run the tool. If you select **IBM WebSphere Application Server - Express**, the embedded version of WebSphere Application Server - Express, V5.0 is installed and configured for you. If you use another

application server, such as Apache Tomcat, you must install the Web Administration Tool file, IDSWebApp.war, into the application server after you install.

This window also indicates the amount of disk space required and available on the selected drive.

Be sure the components you want to install are selected, and click **Next**.

14. The installation program now has enough information to begin installing. A summary window displays the components you selected and the locations where the selected components will be installed. Click **Back** to change any of your selections. Click **Next** to begin installation.
15. After the files are installed, the Client README file opens. Read the file and click **Next**. If you installed the server, the server README file also opens. Read the file and click **Next**.
16. Select to restart your computer now or later. Click **Finish**.

    Note: If you installed the server, you must restart your system to complete the IBM Directory Server configuration. You are unable to use the IBM Directory Server product until this is completed. After the restart, the configuration program runs. The configuration program must complete before you can use the IBM Directory Server. See Chapter 10, "Configuration" on page 63 for more information about using the Configuration Tool to make changes to your configuration at a later time.

You have completed Custom installation and configuration. To see a list of the installed components, click **Start->Programs->IBM Directory Server 5.1**.

After your computer is restarted, if you installed the server, the Configuration Tool automatically runs so that you can complete server configuration. Before you can use the server, you must set the administrator DN and password and configure the database that will store the directory data. To complete configuration, use the following instructions:

1. To set the administrator DN and password, use the instructions in "Setting the Administrator DN and password" on page 64.
2. To configure the database, use the instructions in "Configuring the database" on page 66.

You have completed server configuration.

To make changes to your configuration at a later time, see Chapter 10, "Configuration" on page 63 for more information about using the Configuration Tool.

Before installing on UNIX-based platforms

Note: You cannot migrate from a 3.2.x version of SecureWay Directory or IBM Directory Server 4.1 or reinstall over an existing version of IBM Directory Server 5.1 on a UNIX platform using the InstallShield GUI. See Chapter 3, "Migration from previous releases" on page 17 to install IBM Directory Server if you want to migrate or reinstall.

- **If you have a version of SecureWay Directory installed on your system**, see "Migration from SecureWay Directory Version 3.2.x for AIX installations" on page 20 or "Migration from SecureWay Directory Version 3.2.x for UNIX installations" on page 22.
- **If you have a current or previous version of IBM Directory Server installed on your system**, see "Migration from IBM Directory Server version 4.1 for AIX installations" on page 25 or "Migration from IBM Directory Server Version 4.1 for UNIX installations" on page 25.

Installing IBM Directory Server on a UNIX-based platform

You cannot migrate from a previous version or reinstall over an existing version of the IBM Directory Server 5.1 on an AIX platform using the InstallShield GUI. See Chapter 3, "Migration from previous releases" on page 17 for instructions on migrating and restoring backed-up files after reinstallation on an AIX system.

The InstallShield GUI has two installation options: Typical and Custom. If you want to accept the default settings, select **Typical** during installation. If you are an experienced user and want to customize your installation, select **Custom**.

Typical installation on UNIX-based platforms

Typical installation uses default settings and is recommended for new users.

To install IBM Directory Server 5.1:

1. If you are installing from a CD, insert the CD in the CD-ROM drive. Go to the root directory on your CD. If you downloaded a zip or tar file, go to the directory where you unzipped or untarred the file. Invoke `setup`. A language window is displayed.
2. Select the language you want to use during IBM Directory Server installation. Click **OK**.

   Note: This is the language used in the installation program, not in the IBM Directory Server. You choose the language used in the IBM Directory Server in step 6.
3. On the Welcome window, click **Next**.

Attention: If you have a version of IBM Directory Server already installed on your system, a message is displayed telling you that you must remove it before installing. **If you do not save and back up your data before uninstalling, you will lose it.** See Chapter 3, "Migration from previous releases" on page 17 for information about how to save and back up your data.

4. After reading the Software license agreement, click **I accept the terms in the license agreement** and click **Next**.
5. Any preinstalled components and corresponding version levels are displayed. Click **Next**.
6. Select the language you want to use in IBM Directory Server 5.1. Click **Next**.
7. Click **Typical**. Click **Next**.
8. The following list is displayed:
   - Client SDK 5.1
   - Web Administration 5.1
   - Server 5.1

Notes:

a. If you select **Web Administration 5.1** and embedded version of WebSphere Application Server - Express, V5.0 is not installed, it is installed for you.

b. If you select **Web Administration 5.1**, DSML is also installed. See Appendix E, "Installing and configuring DSML" on page 99 for information about configuring DSML.

Select the features you want to install and click **Next**.

9. A screen summarizing the components selected for installation and configuration is displayed. If you want to change any of your selections, click **Back**. To begin installation, click **Next**.

   Note: Any corequisite products needed by IBM Directory Server, such as DB2, are automatically installed. These products are listed in the summary described in this step.

10. After the files are installed, the Client README file opens. Read the file and click **Next**. If you installed the server, the server README file also opens. Read the file and click **Next**.
11. Click **Finish**. Installation is complete.

If you installed the server, the Configuration Tool automatically runs so that you can complete server configuration. Before you can use the server, you must set the administrator DN and password and configure the database that will store the directory data. To complete configuration, use the following instructions:

1. To set the administrator DN and password, use the instructions in "Setting the Administrator DN and password" on page 64.
2. To configure the database, use the instructions in "Configuring the database" on page 66.

You have completed server configuration.

To make changes to your configuration at a later time, see Chapter 10, "Configuration" on page 63 for more information about using the Configuration Tool.

Custom installation on UNIX-based platforms

Custom installation is for experienced users who want to customize their installations.

To install IBM Directory Server 5.1:

1. If you are installing from a CD, insert the CD in the CD-ROM drive. Go to the root directory on your CD. If you downloaded a zip or tar file, go to the directory where you unzipped or untarred the file.
2. Invoke `setup`. A language window is displayed.
3. Select the language you want to use during IBM Directory Server installation. Click **OK**.

   Note: This is the language used in the installation program, not in the IBM Directory Server. You choose the language used in the IBM Directory Server in step 7 on page 36.

4. On the Welcome window, click **Next**.

Attention: If you have a version of IBM Directory Server already installed on your system, a message is displayed telling you that you must remove it before installing. Before you uninstall, see Chapter 3, "Migration from previous releases" on page 17 for instructions on how to save and back up your data. **If you do not save and back up your data, you will lose it during the uninstall**.

5. After reading the the Software license, select **I accept the terms in the license agreement**. Click **Next**.
6. Any preinstalled components and corresponding version levels are displayed. Click **Next**.
7. Select the language you want to use in IBM Directory Server 5.1. Click **Next**.
8. Click **Custom**.
9. Click **Next**. A window is displayed with the following components:
   - Client SDK 5.1
   - Web Administration 5.1
   - Server 5.1
   - IBM WebSphere Application Server - Express 5.0
   - DB2 V8.1
   - GSKit 6 (SSL packages only.)

   The components that are not yet installed are preselected.

   This window also indicates the amount of disk space required and available on the selected drive.

   Notes:

   a. If you select **Web Administration 5.1**, DSML is also installed. See Appendix E, "Installing and configuring DSML" on page 99 for information about configuring DSML.
   b. If you install the Web Administration Tool, an application server is required to run the tool. If you select **IBM WebSphere Application Server - Express**, the embedded version of WebSphere Application Server - Express, V5.0 is installed and configured for you. If you use another application server, such as Apache Tomcat, or if the embedded version of WebSphere Application Server - Express, V5.0 is already installed, you must, after installation, install the IDSWebApp.war file into the application directory for your application server. For information about installing and configuring embedded version of WebSphere Application Server - Express, V5.0 manually, see Appendix D, "Installing, configuring, and uninstalling embedded version of WebSphere Application Server - Express, V5.0" on page 97.

   Be sure the components you want to install are selected, and click **Next**.
10. The installation program now has enough information to begin installing. A summary panel displays the components you selected and the locations where the selected components will be installed. Click **Back** to change any of your selections. Click **Next** to begin installation.
11. After the files are installed, the Client README file opens. Read the file and click **Next**. If you installed the server, the server README file also opens. Read the file and click **Next**.
12. Click **Finish**. Installation is complete.

If you installed the server, the Configuration Tool automatically runs so that you can complete server configuration. Before you can use the server, you must set the

administrator DN and password and configure the database that will store the directory data. To complete configuration, use the following instructions:

1. To set the administrator DN and password, use the instructions in “Setting the Administrator DN and password” on page 64.
2. To configure the database, use the instructions in “Configuring the database” on page 66.

You have completed server configuration.

To make changes to your configuration at a later time, see Chapter 10, “Configuration” on page 63 for more information about using the Configuration Tool.

Chapter 5. Installing using AIX utilities

You can use either of the following to install the IBM Directory Server on AIX:

- SMIT (This is the preferred installation method.) See "SMIT installation".
- installp. See "Command line installation using installp" on page 41.

Before you install the IBM Directory Server, be sure you have DB2 Version 7.2 FixPak 5 or later installed.

If you are installing the Web Administration Tool, you must install an application server such as the embedded version of WebSphere Application Server - Express, V5.0. See Appendix D, "Installing, configuring, and uninstalling embedded version of WebSphere Application Server - Express, V5.0" on page 97 for information.

Attention: Use SMIT (see "SMIT installation") to install IBM Directory Server if you want to migrate from a 3.2.x version of SecureWay Directory or IBM Directory Server 4.1. Use the appropriate migration process in Chapter 3, "Migration from previous releases" on page 17 before installing the IBM Directory Server. Chapter 3, "Migration from previous releases" on page 17 contains instructions for migrating and restoring backed-up files after reinstallation on an AIX system. It is very important that you back up and export previous versions of schema files and the slapd32.conf file before installing the IBM Directory Server 5.1.

Notes:

1. Full client and server versions require an X11 environment. Versions of IBM Directory Server client and server with no X11 requirements are available in this release. For a client with no X11 requirements, install the minimal client that provides IBM Directory Server Client Runtime (ldap.client.rte) and IBM Directory Server Client SDK (ldap.client.adt).

   For a server with no X11 requirements, do not install the IBM Directory Server Configuration Tool (**ldapxcfg**). **ldapxcfg** is located in the ldap.server.cfg fileset.
2. You do not need to install security functions if you are not going to use them. You can provide SSL by installing a Global Security Kit (GSKit), which is included with IBM Directory Server 5.1.
3. If you are installing the IBM Directory Server on a node within an RS/6000® SP™ environment, see "Before installing on a node within an RS/6000 SP environment" on page 42 before beginning installation.

For more detailed information on AIX operating system installation procedures and commands, see the *AIX Installation Guide* provided with the operating system.

SMIT installation

To install IBM Directory Server using SMIT:

1. Log in as **root**.
2. Insert the CD containing IBM Directory Server 5.1 into the CD-ROM drive or go to the directory where you untarred the file.
3. At the command prompt, type the following:

   ```
   smit install
   ```

and press Enter. The Software Installation and Maintenance window is displayed.

4. Click **Install and Update Software**. The Install and Update Software window is displayed.
5. Click **Install and Update from ALL Available Software**.
6. Click **List** beside the **INPUT device/directory for software** field.
7. Select the appropriate CD-ROM drive or the directory containing the IBM Directory Server images.
8. Move your cursor to **Software to install**. Do one of the following:
   - Type `ldap` to install all the ldap filesets (or ldap.server, or ldap.client, if appropriate).
   - Click **List** to list all the filesets on the CD, and then select the filesets that you want to install, including different translations of IBM Directory Server messages.

     Note: By default SMIT installs translated messages based on the language you configured into your AIX system.

     If you select the list option, you see, for example:

```
> ldap.client                                                 ALL
     5.1.0.0  IBM Directory Client Runtime (No SSL)
     5.1.0.0  IBM Directory Client SDK


> ldap.html.en_US                                             ALL
     5.1.0.0  IBM Directory HTML Install/Config Gd-U.S. English
     5.1.0.0  IBM Directory HTML Man Pages - U.S. English

> ldap.server                                                 ALL
     5.1.0.0  IBM Directory Server Config
     5.1.0.0  IBM Directory Server Framework (No SSL)
     5.1.0.0  IBM Directory Server Java
     5.1.0.0  IBM Directory Server Runtime

> ldap.webadmin                                               ALL
     5.1.0.0  IBM Directory Administrative Interface
```

     Note: The ldap.html packages are language specific. The ldap.html.en_US package is used as an example.

     Select the filesets you want to install and click **OK**.
   - Click **OK**. The message **Are You Sure?** is displayed.
   - Click **OK** to start the installation.
   - Check the installation summary at the end of the output to verify successful installation of the filesets.
   - Click **Done**.
   - To exit SMIT, press F12, or click **Cancel** until you are back to a command prompt. To verify that the IBM Directory Server was installed successfully, type the following at a command prompt:

```
lslpp -L | grep ldap
```

     The output displayed lists all the filesets starting with ldap. This includes the server, client, HTML, and message filesets. For example:

```
ldap.client.adt         5.1.0.0  C  IBM Directory SDK
ldap.client.rte         5.1.0.0  C  IBM Directory Client
ldap.html.en_US.config  5.1.0.0  C  IBM Directory HTML
```

```
ldap.html.en_US.man     5.1.0.0  C  IBM Directory HTML man
ldap.msg.en_US          5.1.0.0  C  IBM Directory Messages
ldap.server.admin       5.1.0.0  C  IBM Directory Server
ldap.server.com         5.1.0.0  C  IBM Directory Server
ldap.server.rte         5.1.0.0  C  IBM Directory Server
ldap.webadmin           5.1.0.0  C  IBM Directory Administrative
```

Command line installation using installp

Note: If you want to migrate from a 3.2.x version of SecureWay Directory or IBM Directory Server 4.1, use the instructions in "SMIT installation" on page 39 to install IBM Directory Server.

To install the IBM Directory Server from a command prompt:

1. Log on as **root**.
2. Insert the CD containing IBM Directory Version 5.1 into the CD-ROM drive or go to the directory where you untarred the file.
3. Determine which IBM Directory Server packages you need. For the server and client, the package name is ldap.server, and for the client only, the package name is ldap.client. For the Web Administration Tool, the package name is ldap.webadmin. For all packages, including all language translations of the message files and documentation, the package name is ldap.
4. Determine which language versions of the message files and documentation you need. To see the language versions that are available, type the following command:

   ```
   installp -ld /dev/cd0 | grep ldap
   ```

   A list of all the installable IBM Directory Server packages is displayed.

   Some examples of United States English-specific packages are:

   ```
   ldap.html.en_US.man
   ldap.msg.en_US
   ```

5. At the command prompt, install the required packages by typing the following command:

   ```
   installp -acgXd /dev/cd0 packages
   ```

   where :

   - **-a** stands for **apply**
   - **-c** stands for **commit**
   - **-g** installs prerequisites if necessary
   - **-X** increases the file system space if needed
   - **-d** stands for **device**

   Examples:

   To install only the IBM Directory Server server and client files, type:

   ```
   installp -acgXd /dev/cd0 ldap.server
   ```

   To install all of the IBM Directory Server filesets (including messages in every available language), type:

   ```
   installp -acgXd /dev/cd0 ldap
   ```

6. Upon completion of installation, the system generates an installation summary. Verify that the Result column shows **success** for all loaded files. You can also verify that the IBM Directory Server was installed successfully by typing the following at a command prompt:

   ```
   lslpp -L | grep ldap
   ```

   The output displayed lists all the filesets starting with ldap. This includes the server, client, HTML, and message filesets. For example:

   ```
   ldap.client.adt         5.1.0.0  C  F   IBM Directory SDK
   ldap.client.rte         5.1.0.0  C  F   IBM Directory Client Runtime
   ldap.server.cfg         5.1.0.0  C  F   IBM Directory Server Config GUI
   ldap.server.com         5.1.0.0  C  F   IBM Directory Server Framework
   ldap.server.java        5.1.0.0  C  F   IBM Directory Server Java
   ldap.server.rte         5.1.0.0  C  F   IBM Directory Server Runtime
   ldap.webadmin           5.1.0.0  C  F   IBM Directory Administrative
   ```

7. If you want to include security functions, install GSKit 6.0.3. See "Installing GSKit".

Before installing on a node within an RS/6000 SP environment

If you are installing the IBM Directory Server on a node within an RS/6000 SP environment you must first add the necessary users and groups to the Control Workstation (CWS) and propagate them out to the nodes using `/var/sysamn/supper` update, as follows:

1. Add ldap user and group on the CWS.

   ```
   mkgroup id=300 ldap
   mkuser id=300 ldap
   chgrpmem -m + ldap ldap
   ```

2. Add the user and the group through the Control Workstation.

   ```
   mkgroup id=350 dbsysadm
   mkuser id=350 ldapdb2
   chgrpmem -m + ldapdb2 dbsysadm
   ```

   Note: The user IDs and group IDs used are just for the purpose of this example. You can choose different user IDs and group IDs for your environment or use the system defaults.

3. Remove the home directory of ldap user.

   ```
   rm -rf /home/ldap
   ```

4. Update the RS/6000 SP nodes with the new users and groups.

   ```
   /var/sysamn/supper update
   ```

You are now ready to install and configure the IBM Directory Server on the RS/6000 SP node.

Installing GSKit

If you installed an SSL-enabled version of IBM Directory Server, you must install GSKit to take advantage of the security features. You can use either SMIT or installp.

To install using SMIT:

1. Invoke SMIT by typing `smit` at the command line.
2. Select **Software Installation & Maintenance**.
3. Select **Install and Update Software**.
4. Select **Install and Update from ALL Available Software**.

5. On the device/directory window specify the directory that contains the installable software.
6. Select **Package gskak** from the multi-select list.
7. Select the filesets of the software packages to install
8. Select the options appropriate to your installation requirements from the Options window.

   Note: Set the **Install all prereqs** option to **yes**.
9. Confirm to complete the installation.

The **installp** command installs available software products in a compatible installation package. To Install GSKit using **installp**, enter the following at a command prompt:

```
installp -acgXd gskak.rte
```

where

- **-a** stands for **apply**
- **-c** stands for **commit**
- **-g** automatically installs or commits any requisite software product.
- **-X** expands the filesystem if necessary.
- **-d** stands for **device**. This specifies where the installation media can be found.

Setting system variables for AIX operating systems

The ikeyman GUI sets up its own environment except for JAVA_HOME. To see how ikeyman sets its environment, edit the /usr/opt/ibm/gskak/bin/gsk6ikm file.

You must set the following AIX variable so that ikeyman can run:
JAVA_HOME=*location*, where *location* is the location where JDK 1.3.1 is installed.

Note: If you are prompted to set JAVA_HOME, you can set it to either the system-installed Java or the Java version included with the IBM Directory Server. If you use the IBM Directory Server version, you also need to set the LIBPATH environment variable as follows:

```
export LIBPATH=/usr/ldap/java/bin:/usr/ldap/java/bin/classic:$LIBPATH
```

Removing GSKit

To remove GSKit using SMIT:

1. Invoke SMIT by typing `smit` at the command line.
2. Select **Software Installation and Maintenance** on the menu.
3. Select **Software Maintenance and Utilities**.
4. On the Maintenance window, select **Remove Installed Software** to open the Remove Software Product window.
5. Enter the name of the software package
6. Set the flag for **REMOVE dependent software?** to **YES** to instruct the system to automatically remove software products and updates that are dependent upon the product you are removing.
7. Confirm the procedure to complete the removal of the software package.

To remove GSKit using **installp**, type the following at a command prompt:

```
installp -u -g -V2 gskak.rte
```

where

- **-u** removes the specified software and any of its installed updates from the system.
- **-g** removes or rejects dependents of the specified software.
- **-V2** prints an alphabetically ordered list of FAILURES and WARNINGS.

Chapter 6. Installing using HP-UX utilities

Attention: If you have IBM Directory Server 4.1 installed, and you want to migrate your data, read and understand the migration process in "Migration from IBM Directory Server Version 4.1 for UNIX installations" on page 25 before installing IBM Directory Server 5.1. It is very important that you back up and export previous versions of schema files and the slapd32.conf file before installing IBM Directory Server 5.1.

Before installing the IBM Directory Server

The following sections step you through setting the current configuration parameters and installing the Java Runtime Environment. You must have the current kernel configuration parameters set, and Java Runtime Environment 1.3.1 and DB2 Version 7.2 FixPak 5 or later installed before installing the IBM Directory Server.

If you are installing the Web Administration Tool, you must install an application server such as Apache Tomcat. You can obtain Apache Tomcat from the Apache Web site.

Instructions given in this chapter assume you are logged in as **root** and have the IBM Directory Server Version 5.1 CD mounted at /SD_CDROM.

Note: Before installing DB2, you must remove any existing versions of DB2 that might have been installed previously. If you try to install DB2 over an existing version of DB2, DB2 does not install correctly. If this occurs you must remove DB2 and then reinstall it.

Setting the current kernel configuration parameters

The following table contains the parameters and values that must be set before installing IBM Directory Server.

Table 1. HP-UX operating system kernel configuration parameters

Kernel parameter	Value 256MB+ physical memory
maxuprc	512
maxfiles	256
nproc	1024
nflocks	8192
ninode	2048
nfile	(4 * ninode)
msgseg	32768
msgmnb	65535 (1)
msgmax	65535 (1)
msgtql	1024
msgmap	258

Table 1. HP-UX operating system kernel configuration parameters (continued)

Kernel parameter	Value 256MB+ physical memory
msgmni	256
msgssz	16
semmni	512
semmap	514
semmns	1024
semmnu	1024
shmmax	268435456 (2)
shmseg	16
shmmni	300
max_thread_proc (Only if using the Web Administration Tool)	1024
maxusers (Only if using the Web Administration Tool)	256

Note: After you update the max_thread_proc and maxusers parameters, be sure that the nproc parameter is set to 2068 or more, and the nkthread parameter to 3635 or more.

To set a kernel configuration parameter:

1. At a command prompt, type: `sam`
   The System Administration Manager opens.
2. Double-click **Kernel Configuration**.
3. Double-click **Configurable Parameters**.
4. Double-click the parameter you want to edit and specify the new value in the **Enter New Formula/Value** field. Click **OK**.
5. Repeat step 4 for each parameter that needs to be set.
6. Click **Actions-->Process New Kernel**.
7. To process the modifications, click **Yes**.
8. Select **Move Kernel Into Place and Shutdown/Reboot Now** and click **OK**.

Installing HP-UX Runtime Environment for the Java 2 Platform Version 1.3.1

Do the following to install HP-UX Runtime Environment for the Java 2 Platform Version 1.3.1:

1. Download or copy the Java package to a directory.
2. Change to the directory where the Java package is located.
3. Type `swinstall` at a command prompt.
4. Select **B9789AA**
5. Click **Actions –>Mark For Install**.
6. Click **Actions –>Install (analysis)**. Analysis is complete when the **Status** field reads **Ready**.

7. Click **OK**.
8. To begin installation, click **Yes**. Installation is complete when the **Status** field reads **Done**.
9. Click **File --> Exit**.

Installing the IBM Directory Server

Before installing the IBM Directory Server, you must remove any non-IBM versions of LDAP that might have been installed previously. If you try to install the IBM Directory Server over an existing non-IBM version of LDAP, such as OpenLDAP, the IBM Directory Server might not install correctly. If this occurs you must remove the IBM Directory Server and then reinstall it. See "Uninstalling IBM Directory Server" on page 77.

Before installing the IBM Directory Server, make sure you have the correct kernel configuration parameters set, and Java Runtime Environment 1.3.1 and DB2 Version 7.2 FixPak 5 or later installed.

To install the IBM Directory Server:

1. Type `swinstall` at a command prompt.
2. Select the IBM Directory Server 5.1 package you want to install. You can select from the following list:
   - **LDAPServer** to install both the server and client.
   - **LDAPClient** to install the client only.
   - **LDAPServer_noSSL** to install the client and server with SSL disabled.
   - **LDAPClient_noSSL** to install the client only with SSL disabled.
   - **ids_tools** to install the Web Administration Tool.

   Note: If you select an SSL-enabled version of IBM Directory Server, you must also install GSKit to enable SSL. See "Installing GSKit".
3. Click **Actions -->Mark For Install**.
4. Click **Actions -->Install (analysis)**. Analysis is complete when the Status field reads **Ready**.
5. Click **OK**.
6. Click **Yes** to begin installation. Installation is complete when the Status field reads **Done**.
7. Click **File --> Exit**.

Installing GSKit

You can install the GSKit package (gsk6bas.tar.Z) through the command line or through **sam**, a GUI utility for system administration.

To install GSKit:

1. Download or copy the GSKit package to /tmp.
2. Run the following command to change to the /tmp directory:
   ```
   cd /tmp
   ```
3. Uncompress and untar the package:
   ```
   zcat gsk6bas.tar.Z | tar -xvf - cd
   ```
4. Run the following command to install:
   ```
   swinstall  -s /var/spool/pkg/gsk6bas gsk6bas
   ```

where

- **-s** specifies the full_path of the software source.
- **gsk6bas** contains the Restricted GSKit Base Toolkit install image.

Setting system variables for HP-UX

Set or verify that the following path has been set in your `.profile`.

```
SHLIB_PATH=/usr/lib
```

For example:

```
export SHLIB_PATH=/usr/lib;$SHLIB_PATH
```

To set the NLS environment variables, run the following command:

```
echo 'export NLSPATH=/usr/lib/nls/msg/%L/%N' >>~/.profile
```

Note: Be sure to include the tilde character before `/.profile`.

Removing GSKit

To remove GSKit, run the following command at a command prompt:

```
swremove gsk6bas
```

Chapter 7. Installing using Linux utilities

Instructions given in this chapter assume you are logged in as **root** and have the IBM Directory Server Version 5.1 CD mounted at /SD_CDROM.

Attention: If you have SecureWay Directory version 3.1.1.5, 3.2,. 3.2.1, or 3.2.2, or IBM Directory Server 4.1 installed, and you want to migrate your data, use the instructions in Chapter 3, "Migration from previous releases" on page 17 to install IBM Directory Server 5.1. It is very important that you back up and export previous versions of schema files and the slapd32.conf file before installing IBM Directory Server 5.1.

Installing the IBM Directory Server

Note: Before installing the IBM Directory Server, you must remove any existing versions of LDAP that might have been installed previously. If you try to install the IBM Directory Server over an existing version of LDAP, the IBM Directory Server does not install correctly. If this occurs you must remove the IBM Directory Server and then reinstall it. See "Uninstalling IBM Directory Server" on page 77.

One method to determine if you have a previously installed version of LDAP is to issue the following command to query the installed packages:

```
rpm -qa | grep -i ldap
```

This command finds any installed applications containing the name ldap. This method works only if you have a version of LDAP that contains the string ldap in its application names.

Before you install the IBM Directory Server, be sure you have DB2 Version 7.2 FixPak 5 or later installed.

If you are installing the Web Administration Tool, you must install an application server such as the embedded version of WebSphere Application Server - Express, V5.0. See Appendix D, "Installing, configuring, and uninstalling embedded version of WebSphere Application Server - Express, V5.0" on page 97 for information.

The IBM Directory Server for the Linux operating system is provided in the following packages.

Intel-based Linux packages:

- ldap-server-5.1-1.i386.rpm (no SSL)
- ldap-client-5.1-1.i386.rpm (no SSL)
- ldap-serverd-5.1-1.i386.rpm (SSL enabled)
- ldap-clientd-5.1-1.i386.rpm (SSL enabled)
- ldap-msg-*xxx*-5.1-1.i386.rpm (Where *xxx* is language dependent.)
- ldap-html-*xxx*-5.1-1.i386.rpm (Where *xxx* is language dependent.)
- ldap-webadmin-5.1-1.i386.rpm (No SSL)
- ldap-webadmind-5.1-1.i386.rpm (SSL enabled)

Linux for S/390 packages:

- ldap-server-5.1-1.s390.rpm (no SSL)
- ldap-client-5.1-1.s390.rpm (no SSL)
- ldap-serverd-5.1-1.s390.rpm (SSL enabled)
- ldap-clientd-5.1-1.s390.rpm (SSL enabled)
- ldap-msg-*xxx*-5.1-1.s390.rpm (Where *xxx* is language dependent.)
- ldap-html-*xxx*-5.1-1.s390.rpm (Where *xxx* is language dependent.)
- ldap-webadmin-5.1-1.s390.rpm (No SSL)
- ldap-webadmind-5.1-1.s390.rpm (SSL enabled)

Note: The examples in this chapter use Linux Intel-based packages.

To install the IBM Directory Server with no SSL:

1. Install the client by typing the following at a command prompt:

   ```
   rpm -ihv ldap-client-5.1-1.i386.rpm
   ```

2. Install the server by typing the following at a command prompt:

   ```
   rpm -ihv ldap-server-5.1-1.i386.rpm
   ```

3. Verify that the packages have been installed correctly by typing the following at a command prompt:

   ```
   rpm -qa | grep ldap
   ```

   If the product has been successfully installed, the following is displayed:

   ```
   ldap-client-5.1-1
   ldap-server-5.1.1
   ```

4. Install the language-dependent messages or documents by typing the following at a command prompt:

   ```
   rpm -ihv ldap-msg-xxx-5.1-1.i386.rpm
   rpm -ihv ldap-html-xxx-5.1-1.i386.rpm
   ```

To install the IBM Directory Server with SSL enabled:

1. Install the client by typing the following at a command prompt:

   ```
   rpm -ihv ldap-clientd-5.1-1.i386.rpm
   ```

2. Install the server by typing the following at a command prompt:

   ```
   rpm -ihv ldap-serverd-5.1-1.i386.rpm
   ```

3. Verify that the packages have been installed correctly by typing the following at a command prompt:

   ```
   rpm -qa | grep ldap
   ```

   If the product has been successfully installed, the following is displayed:

   ```
   ldap-clientd-5.1-1
   ldap-serverd-5.1.1
   ```

4. Install the language-dependent messages or documents by typing the following at a command prompt:

   ```
   rpm -ihv ldap-msg-xxx-5.1-1.i386.rpm
   rpm -ihv ldap-html-xxx-5.1-1.i386.rpm
   ```

To install the Web Administration Tool with no SSL:

1. Type the following at a command prompt:

   ```
   rpm -ihv ldap-webadmin-5.1-1.i386.rpm
   ```

To install the Web Administration Tool with SSL enabled:

1. Type the following at a command prompt:

   ```
   rpm -ihv ldap-webadmind-5.1-1.i386.rpm
   ```

Installing GSKit

The following information is provided as a guide if you want to install the software package gsk6bas.tar on the Linux operating system. You can install the package through the command line.

The rpm commands to perform the installation are as follows:

- To install in the default location, /usr/local, log in as **root** and type the following at a command prompt:

  ```
  rpm -ihv gsk6bas-6.0-3.23.i386.rpm
  ```

- To install in a specified location, be sure that you have write access to the directory and use the --noscripts flag, as follows:

  ```
  rpm -ihv --prefix new_location gsk6bas-6.0-3.23.i386.rpm --noscripts
  ```

  where *new_location* is the path where you want to install. For example:

  ```
  rpm -ihv --prefix /tmp/usr gsk6bas-6.0-3.23.i386.rpm --noscripts
  ```

Removing GSKit

To remove GSKit, type the following at a command prompt:

```
rpm -evv gsk6bas-6.0.1
```

where

- **-evv** specifies to erase the package and display debugging information. If no trace or debug information is desired, use only **-e**.

Chapter 8. Installing using Solaris utilities

Instructions given in this chapter assume you are logged in as **root** and have the IBM Directory Server Version 5.1 CD in the CD-ROM drive.

Attention: If you have a 3.2.x version of SecureWay Directory or IBM Directory Server 4.1 installed, and you want to migrate your data, use the instructions in Chapter 3, "Migration from previous releases" on page 17 to install IBM Directory Server 5.1. It is very important that you back up and export previous versions of schema files and ibmslapd.conf before installing IBM Directory Server 5.1.

Before you install on Solaris

Note: Before installing the IBM Directory Server, you must remove any existing versions of LDAP that might have been installed previously. If you try to install the IBM Directory Server over an existing version of LDAP, the IBM Directory Server does not install correctly. See "Uninstalling IBM Directory Server" on page 77.

Before you install the IBM Directory Server, be sure you have DB2 Version 7.2 FixPak 5 or later installed.

Note: If you use DB2 8.1, update the /etc/system file with the following values before you configure the database.

```
set msgsys:msginfo_msgmax = 65535
set msgsys:msginfo_msgmnb = 65535
set msgsys:msginfo_msgmap = 258
set msgsys:msginfo_msgmni = 256
set msgsys:msginfo_msgssz = 16
set msgsys:msginfo_msgtql = 512
set msgsys:msginfo_msgseg = 32768
set shmsys:shminfo_shmmax = 268435456
set shmsys:shminfo_shmseg = 32
set shmsys:shminfo_shmmni = 300
set semsys:seminfo_semmni = 512
set semsys:seminfo_semmap = 514
set semsys:seminfo_semmns = 1024
set semsys:seminfo_semmnu = 1024
set max_nprocs=65535
set maxuprc=65535
```

See the DB2 documentation for more information about these parameters.

If you are installing the Web Administration Tool, you must install an application server such as the embedded version of WebSphere Application Server - Express, V5.0. See Appendix D, "Installing, configuring, and uninstalling embedded version of WebSphere Application Server - Express, V5.0" on page 97 for information.

Installing on Solaris

You can use either the **admintool** utility or **pkgadd** from a command prompt to install IBM Directory Server.

Note: You do not need to install security functions if you are not going to use them. You can provide SSL by installing a Global Security Kit (GSKit).

The following instructions assume that you are installing from a CD-ROM drive.

Package dependencies

The following IBM Directory Server packages are available for installation:

- IBMldapc: IBM Directory Server client
- IBMldaps: IBM Directory Server server
- IBMldixxx: IBM Directory Server documentation (where xxx is language dependent)
- IBMldmxxx: IBM Directory Server messages (where xxx is language dependent)
- IBMldapw: IBM Directory Server Web Administration Tool

Note: The English messages are automatically installed with the IBMldaps (server) package. There is no separate messages package for English.

Because of package dependencies, the order of installation is significant. Install the packages in the following order:

1. Client
2. Server
3. Documentation and Messages

If installing only the client software, the order is:

1. Client
2. Documentation and Messages

If the client package is not installed first, the installation fails.

Note: Because the Web Administration Tool package has no dependencies on any of the other packages, and none of the other packages are dependent on it, you can install it in any order.

Non-IBM version of LDAP on your system

During the installation of the server or client on Solaris Operating Environment Software Version 8 or 9, or the server on Version 7, you might encounter the following message:

```
A non-IBM version of LDAP has been located on your system. In order
to use the command line version of the IBM supplied files, the
existing files (ldapadd, ldapdelete, ldaplist, ldapmodify,
ldapmodrdn,  ldapsearch) must be relocated.  Specify the new
directory in which to move the files (/usr/bin/ldapsparc) [?,q]
```

Press Enter to accept the default directory (/usr/bin/ldapsparc), or type a new path name and press Enter, or type `q` and press Enter to quit.

After relocating the files, you might see these additional messages:

```
## Processing system information.
WARNING: /usr/bin/ldapadd <no longer a linked file>
WARNING: /usr/bin/ldapdelete <no longer a linked file>
WARNING: /usr/bin/ldapmodify <no longer a linked file>
WARNING: /usr/bin/ldapmodrdn <no longer a linked file>
WARNING: /usr/bin/ldapsearch <no longer a linked file>
## Verifying package dependencies.
```

```
## Verifying disk space requirements.
## Checking for conflicts with packages already installed.

The following files are already installed on the system and
are being used by another package:
/usr/bin/ldapadd
/usr/bin/ldapdelete
/usr/bin/ldapmodify
/usr/bin/ldapmodrdn
/usr/bin/ldapsearch

Do you want to install these conflicting files [y,n,?,q]
```

Type y and press Enter to continue the installation. The existing files are moved to the directory previously specified and the IBM Directory Server files are installed in the /usr/bin directory.

AdminTool installation

To install IBM Directory Server using the **admintool** utility:

1. Type the following at a root command prompt: admintool&

   The Users window is displayed.
2. Click **Browse--> Software**. The Software window is displayed.
3. Click **Edit--> Add**. The Set Source Media window is displayed.

   Attention: Do not click **Customize** in the lower left corner of the Set Source Media window. If you click **Customize**, AdminTool crashes. Because LDAP does not have any customizable options, there is no need for you to click **Customize**.
4. Select **CD with Volume Management**. The CD-ROM path defaults to: /cdrom/cdrom0/
5. Change the path to /cdrom/cdrom0/ldap51_us and click **OK**.
6. Click **OK**.
7. Select from the following list of installable packages:

   ```
   IBM Directory Client
   IBM Directory Server
   IBM Directory Documentation (for all languages)
   IBM Directory Messages (for all languages)
   IBM Directory Webadmin
   ```

   Remember that you must install the IBMldapc package first. See “Package dependencies” on page 54 for the correct installation sequence.
8. Click **Add**.
9. You are asked if you want to use /opt as the base directory. If space permits, use /opt as the base installation directory. To accept /opt as the base directory, press Enter.

   Notes:

   a. With the installation of client and server packages, the system prompts you with the notice, This package contains scripts which will be executed with super-user permission during the process of installing the package. These scripts create the IBM Directory Server user ID. Type y to continue.

   b. If you are installing the server package, you also see the prompt, Do you want to install these as setuid/setgid files? Type y to continue.

After the package is installed, the Software window is displayed.

10. Repeat steps 7 on page 55 through 9 on page 55 for each additional package you want to install. If you are finished installing the packages, select **File--> Exit** to exit the **admintool** utility.

Command line installation using pkgadd

To install the IBM Directory Server from a command prompt:

1. At the command prompt, install the packages you want by typing the following command:

   ```
   pkgadd -d /cdrom/cdrom0/ldap51_us pkglist
   ```

   where *pkglist* is the list of packages you want to install. Do not use the system default of **ALL**. The system does not sequence the packages correctly and the installation fails.

   The following packages are available:

   ```
   IBMldapc    IBM Directory Client
   (sparc) 5.1.0.0
   IBMldaps     IBM Directory Server
   (sparc) 5.1.0.0
   IBMldixxx    IBM Directory documentation
   (sparc) 5.1.0.0
   IBMldmxxx    IBM Directory messages
   (sparc) 5.1.0.0
   IBMldapw     IBM Directory Webadmin
   (sparc) 5.1.0.0
   ```

   where *xxx* is a specific language identifier.

   Note: The English messages are automatically installed with the IBMldaps (server) package. There is no separate package for English messages.

   Examples:

   - To install all IBM Directory Server packages, enter:

     ```
     pkgadd -d /cdrom/cdrom0/ldap51 IBMldapc IBMldaps IBMldixxx IBMldmxxx IBMldapw
     ```

     Note: The order in which the packages are listed is crucial, with the exception of the Web Administration Tool package. If package dependencies are not met, the installation fails.

   - To install the client only, enter:

     ```
     pkgadd -d /cdrom/cdrom0/ldap51 IBMldapc
     ```

   - To install the client and documentation packages, enter:

     ```
     pkgadd -d /cdrom/cdrom0/ldap51 IBMldapc IBMldixxx
     ```

   - To install the client and server packages, enter:

     ```
     pkgadd -d /cdrom/cdrom0/ldap51 IBMldapc IBMldaps
     ```

   - To install the client, server, and message packages, enter:

     ```
     pkgadd -d /cdrom/cdrom0/ldap51 IBMldapc IBMldaps IBMldmxxx
     ```

   - To install the Web Administration Tool package, enter:

     ```
     pkgadd -d /cdrom/cdrom0/ldap51 IBMldapw
     ```

2. During installation, you are asked if you want to use `/opt` as the base directory. If space permits, use `/opt` as the base installation directory. To accept `/opt` as the base directory, press Enter.

Notes:

a. With the installation of client and server packages, the system prompts you with the query, `This package contains scripts which will be executed with super-user permission during the process of installing the package. Continue with installation?` These scripts create the IBM Directory Server user ID. Type `y` to continue.

b. If you are installing the server package, you also see the prompt, `Do you want to install these as setuid and/or setgid files?` The programs need to be able to start daemons, run DB2 commands, and create the IBM Directory Server DB2 instance user ID and group, so they occasionally need to run as root. Type `y` to continue.

3. When the installation is completed, type `q` to return to the command prompt.

Installing GSKit

You can install GSKit 6 using either the AdminTool or the command line.

To install the IBM Directory Server using the **admintool** utility:

1. Log in as **root**.
2. Type the following at a root command prompt: `admintool&`
   The Users window is displayed.
3. Click **Browse--> Software**. The Software window is displayed.
4. Click **Edit--> Add**. The Set Source Media window is displayed.
5. Type the full path name to the directory that contains the GSKit installation code in the **Path** field. For example, if you are installing from a CD-ROM :
   `/cdrom/cdrom0/gskit`
6. Click **OK**.
7. Select **Certificate and SSL Base Runtime (gsk6bas)**
8. Click **Add**. You are asked if you want to continue the installation.
9. Type `y` and press Enter. After the package is installed, a message is displayed and you are instructed to press Return.
10. Press Enter.
11. When you are finished installing packages, click **File-->Exit** to exit the **admintool** utility.

To install GSKit using the command line:

1. Insert the CD.
2. Log in as **root**.
3. At the command prompt, install the required tar file sets with the following command:
   `pkgadd -d /cdrom/cdrom0/gskit`

Removing GSKit

To remove GSKit, type the following at a command prompt:

`pkgrm gsk6bas`

Chapter 9. Installing using Windows utilities

This chapter provides instructions for installing IBM Directory Server 5.1 on a Windows computer using silent installation, and for installing and uninstalling GSKit from the command line on Windows.

Silent installation

Silent installation installs the IBM Directory Server with no user input required during installation.

The following options and conditions apply to silent installation:

- You must have at least 100 MB available memory before invoking silent installation.
- You do not need to install both the client and the server. You can choose to install the client only.
- Silent installation does not install GSKit or the embedded version of WebSphere Application Server - Express, V5.0.
- If you choose to install the server, you must already have DB2 installed.
- If the client is already installed, you can add the server in a later installation.
- If the server is selected for installation in the options file, the client will automatically be installed if it is not there, regardless of whether it was selected for installation in the options file.
- The Web Administration Tool can be installed whether or not the server or client is installed.
- To edit installation path settings, copy the InstallServer.txt file from the optionsFile directory to a writable location.
- After installation and restart, if the server was installed, you must configure before the server is usable. You can use the **ldapcfg** command line utility to configure silently. See "Using the ldapcfg utility" on page 71 for information.

To begin installing the IBM Directory Server 5.1 using silent installation:

1. If you are installing from the CD, insert the CD in your CD-ROM drive.
2. At a command prompt, type the following:

   ```
   d:
   cd \ismp
   setup -is:silent -options d:\ismp\optionsFiles\InstallServer.txt
   ```

   where *d:* is the CD-ROM drive or the drive from which you are installing the IBM Directory Server.
3. To specify an additional log file, type the following:

   ```
   setup -is:silent -options d:\ismp\optionsFiles\InstallServer.txt -log
       !c:\mydirectory\ldapinst.log @ALL
   ```

   c:\mydirectory\ldapinst.log can be changed to point to where you want to place the log file. The log file will still get created in the target installation directory. The default location is C:\Program Files\IBM\LDAP\ldapinst.log.

IBM Directory Server is installed with no further input. If installation exits for any reason, you can find information about the exit in the *installpath*\ldapinst.log file.

Installation is complete when the last log entry in the *installpath*\ldap\ldapinst.log reads: **Exiting LdapExit**.

installpath is the path where you installed IBM Directory Server.

If installation is unsuccessful, check to be sure that your options file settings and command line parameters are valid.

Verifying the silent installation

To verify that silent installation was successful:

1. Check the log file to see if it exists in the target directory. If the log is not there, the installation failed, and you can refer to the log file that was specified on the silent installation command with the **-log** option to see why the installation failed.
2. Check the log file for the string **Exiting LdapExit**.
3. Verify the install was complete by checking the Windows registry. The following should be in the registry, depending on which components were installed:

```
HKEY_LOCAL_MACHINE\SOFTWARE\IBM\LDAP\ClientMajorVersion 5.1
                                    ServerMajorVersion 5.1
                                    WebadminMajorVersion 5.1
```

Common reasons for the silent installation failing are:

- A previous or current version of IBM Directory Server is already installed.
- The prerequisites are not present. The server requires a valid version of DB2.
- There is not enough disk space to install.
- The options file is incorrect. Be very careful when editing the options file. There should be no blank lines and no control characters in the file. If the installation exits with no log file, this is usually caused by an invalid options file (with blank lines, for example), or by incorrectly specifying the path to the options file.

Options file for silent installation

The following is the options file provided with the IBM Directory Server:

```
#Sample response file for the Server/Client package
#(Lines beginning with # are comments)
# Be sure there are no blank lines in this file!
#
# The following 3 lines MUST be present, and NOT modified
-silent
-G createDirectoryResponse="yes"
-G replaceExistingResponse="yesToAll"
#
# install destination - this can be modified to install location
-P product.installLocation="C:\Program Files\IBM\ldap"
#
# Select the features to install. Note: if the server is selected, the
# client will automatically be installed. To deselect a feature, set the
# field to false.
-P ServerFeature.active=true
-P ClientFeature.active=true
-P WebadminFeature.active=true
# This must be last line. Be sure no blank lines or carriage controls follow!
```

The line `-P product.installLocation="C:\Program Files\IBM\ldap"` can be edited to point to the desired target installation directory.

The features lines can be edited to disable a feature from being installed. For instance, `-P WebadminFeature.active=true` can be changed to `-P WebadminFeature.active=false` to indicate that you do not want to install the IBM Directory Server Web Administration Tool.

Installing GSKit on Windows operating systems

If you install the IBM Directory Server using silent installation, GSKit is not installed. You can use the following procedure to install it.

To install GSKit 6:

1. To extract the files from the self-extracting GSKit file, type the following at a command prompt in the directory where the gsk6bas.exe file is located:

   `gsk6bas.exe` *`path`* `/D`

   where

   - *path* is the directory you want to extract the files to
   - /D specifies that you want to create directories
2. At a command prompt, run the following command:

   `setup LDAP` *`path`* `-s -f1"`*`extracted file location`*`\setup.iss"`

   where

   - LDAP is the name of your application and will be registered as a registered user of GSK in the Windows Registry (under the key SOFTWARE\\IBM\\GSK\\REGAPPS).
   - *path* is the path where you want to install GSKit. Note that the installation program appends \ibm\gsk6 to any path you enter.

     Note: Do not start setup.exe by clicking on the icon.

   The following options can be used:

   - **-s** to run the setup in the silent mode.
   - **-f1***extracted file location*\setup.iss specifies the response file needed to run the setup in the silent mode. Note that there is no space between **-f1** and the beginning of the extracted file location.

For example:

```
setup LDAP gskit -s -f1"d:\temp\setup.iss"
```

Removing GSKit

To remove GSKit, run the following command:

```
gsk6BUI LDAP
```

Chapter 10. Configuration

You can use either the Configuration Tool (**ldapxcfg**) or the **ldapcfg** command-line utility to configure the server. **ldapucfg** is used to unconfigure through the command line.

Note: The Configuration Tool cannot be used on HP-UX Traditional Chinese systems.

You must have at least 80 MB of hard disk space available to configure.

If you used the InstallShield GUI to install, the Configuration Tool is started after installation (and after system restart on a Windows system).

After installation, if configuration was not started automatically, you must use the Configuration Tool or the command line configuration program to do the following tasks:

- Define the IBM Directory Server administrator distinguished name (DN) and a password. This operation can be compared to defining the root user ID and password on a UNIX system.
- Configure the database.

  Note: After you configure, see the *IBM Directory Server version 5.1 Administration Guide* for information about:
  - Starting the server
  - Starting the embedded version of WebSphere Application Server - Express, V5.0 service if you want to use the Web Administration Tool

In addition, you can use the Configuration Tool for the following tasks:

- Configuring (or reconfiguring) and unconfiguring the database
- Enabling and disabling the change log
- Adding and removing suffixes
- Adding and removing schema files
- Importing and exporting LDIF data
- Backing up, restoring, and optimizing the database

Note: If you are configuring a UNIX-based system, you must run the configuration utilities (**ldapcfg** and **ldapxcfg** from a directory that has execute permission for **other**. That is, the directory must have at least the **--------x** permission set. If this permission is not set, you might see an error message and experience a subsequent failure during the database creation step. To set this permission for your current directory, you can enter the command:

```
chmod o+x .
```

The period (.) in the command is required to indicate the current directory.

Using the IBM Directory Server Configuration Tool (ldapxcfg)

To configure the IBM Directory Server using the Configuration Tool:

1. On a UNIX system, log in as **root**. On a Windows system, log on as any user in the Administrators group.
2. Type `ldapxcfg` at a command prompt. Alternatively, on a Windows system, you can click **Start -> Programs -> IBM Directory Server 5.1 -> Directory Configuration**.
3. The Configuration Tool window is displayed.

   Note: If you are using a Windows platform, do not minimize the Configuration Tool window or the command prompt window that is displayed during initial configuration, or unpredictable results might occur.

   In the task list on the left, click the task you want to perform. For information about performing a task, see the section shown in the following list:

   Set or change the Administrator DN and password
   See "Setting the Administrator DN and password".

   Configure the database
   See "Configuring the database" on page 66.

   Unconfigure the database
   See "Unconfiguring the database" on page 67.

   Configure or unconfigure the change log
   See "Enabling or disabling the change log" on page 67.

   Manage suffixes
   See "Managing suffixes" on page 68.

   Manage schema files
   See "Managing schema files" on page 68.

   Import LDIF data
   See "Importing LDIF data" on page 70.

   Export LDIF data
   See "Exporting LDIF data" on page 70.

   Back up database
   See "Backing up the database" on page 71.

   Restore database
   See "Restoring the database" on page 71.

   Optimize database
   See "Optimizing the database" on page 71.
4. Close the Configuration Tool when you have completed all configuration tasks.

Setting the Administrator DN and password

To set the administrator DN and password:

1. In the IBM Directory Server Configuration Tool window, click **Administrator DN/password** in the task list on the left.
2. In the Administrator DN/password window on the right, type a valid DN (or accept the default DN) in the **Administrator DN** field.

   The IBM Directory Server administrator DN is the DN used by the administrator of the directory. This is the one user who has full access to all data in the directory.

The default DN is **cn=root**. DNs are not case sensitive. If you are unfamiliar with X.500 format, or if for any other reason you do not want to define a new DN, accept the default DN.

3. Type the password for the Administrator DN in the **Administrator Password** field. You must define a password. Passwords are case-sensitive.

   Record the password for future reference.
4. Retype the password in the **Confirm password** field.
5. Click **OK**.

Configuring or unconfiguring the database

When you configure the database, the Configuration Tool adds information about the database that will be used to store directory data to the configuration file (ibmslapd.conf). In addition, if the database does not already exist, the Configuration Tool creates the database.

Notes:

1. Before configuring the database, be sure that the environment variable DB2COMM is **not** set.
2. If you are using DB2 8.1 on Solaris, read the information in "Before you install on Solaris" on page 53 before you configure the database.

When you unconfigure the database, the Configuration Tool removes the database information from the configuration file. Based on your selections, it might also delete the database (and all data in it) and remove the instance that contains the database.

Before you configure: creating the DB2 database owner

Before you configure the database, you must create a user ID for the user who will own the DB2 database. The user ID you specify will own the database instance where the DB2 database will exist, and the DB2 instance will be in the user's home directory. The user ID can be no longer than 8 characters. In addition:

- On Windows platforms, the user must be a member of the Administrators group.
- On UNIX platforms:
  - The user's Primary group can be any general group (such as **other**, **dbsysadm**, or **db2iadm**). There might be some groups that do not work correctly as the user's primary group when configuring the database. For example, if the user's primary group on Linux is **users**, problems might occur. Use **other** if you want to be sure that the Primary group will work.
  - The user **root** must be a member of the user's primary group. If **root** is not a member of this group, add **root** as a member of the group.
  - For best results, the user's login shell should be the Korn shell script (/usr/bin/ksh).
  - The user's password must be set correctly and ready to use. For example, the password cannot be expired or waiting for a first-time validation of any kind. (The best way to verify that the password is correctly set is to telnet to the same computer and successfully log in with that user ID and password.)
  - The user must have a home directory and must be the owner of the home directory.
  - The group ownership of the user's home directory must be the user's primary group.

– When configuring the database, it is not necessary, but only customary, to specify the home directory of the user ID as the database location. However, if you specify some other location, the user's home directory still must have 3 to 4 MB of space available. This is because DB2 creates links and adds files into the home directory of the instance owner (that is, the User) even though the database itself is elsewhere.

Configuring the database

To configure the directory database:

1. In the Configuration Tool, click **Configure database** in the task list on the left.
2. The Configuration Tool attempts to determine whether you already have a database. If you have a database already configured (that is, the information for the database is in the configuration file), the Configuration Tool prompts you for information about what you want to do. For example, if the database is configured but cannot be found on the system, you might choose to create a database using the name specified in the configuration file. Use the information shown in the windows that are displayed to configure the database.

Depending on whether or not you already have a database, some or all of the following windows are displayed.

3. If a window is displayed requesting a user ID and password:
   a. Type a user ID in the **User ID** field. This user ID must already exist before you can configure the database. This is the user ID you created in "Before you configure: creating the DB2 database owner" on page 65. (In previous releases, the user ID was created if it did not exist, but this is no longer true.)
   b. Type a password for the user in the **Password** field. Passwords are case-sensitive.
   c. Click **Next**.
4. If a window is displayed requesting the database name:
   a. Type the name you want to give the DB2 database. The name can be from 1 to 8 characters long. The database will be created in an instance with the same name as the user ID.
   b. Click **Next**.
5. If a window is displayed requesting the database location:
   a. Type the location for the database in the **Database location** field. For Windows platforms, this must be a drive letter. For non-Windows platforms, the location must be a directory name, such as /home/ldapdb2.

      Be sure that you have at least 80 MB of free hard disk space in the location you specify and that additional disk space is available to accommodate growth as new entries are added to the directory.
   b. Click **Next**.
6. If a window is displayed requesting you to choose a character set:
   a. Click the type of database you want to create. You can create a UCS Transformation Format (UTF-8) database, in which LDAP clients can store UTF-8 character data, or a local code page database, which is a database in the local code page.

      For more information about UTF-8, see Appendix F, "UTF-8 support" on page 101.
   b. Click **Next**.

7. In the verification window, information is displayed about the configuration options you specified. To return to an earlier window and change information, click **Back**. To begin configuration, click **Finish**.
8. The completion window is displayed. Click **Close**.

Unconfiguring the database

To unconfigure the database:

1. In the Configuration Tool, click **Unconfigure database** in the task list on the left.
2. In the Unconfigure database window, click one of the following:

   Unconfigure only
   Does not destroy any existing LDAP DB2 data. However, the configuration information for the database will be removed from the configuration file (ibmslapd.conf), and the database will be inaccessible to the directory server.

   Unconfigure and destroy database
   Removes the existing database and its contents, and removes the configuration information for the database from the configuration file.

   Unconfigure and destroy database and delete instance
   Removes the existing database and its contents, removes the configuration information for the database from the configuration file, and deletes the instance in which the database is located.

   Warning: Before destroying an instance, be sure that there are no databases in the instance that must be kept.
3. Click **Unconfigure**.

Enabling or disabling the change log

The change log database is used to record changes to the schema or directory entries in the typical LDAP entry structure that can be retrieved through the LDAP API. The change log records all update operations: add, delete, modify, and modrdn. The change log enables an IBM Directory Server client application to retrieve a set of changes that have been made to an IBM Directory Server database. The client might then update its own replicated or cached copy of the data.

You can use the Configuration Tool to enable or disable the change log.

Enabling the change log

To enable the change log:

1. In the Configuration Tool, click **Configure/unconfigure changelog** in the task list on the left.
2. In the Configure/unconfigure changelog window, select the **Enable change log database** check box.
3. Type the maximum number of entries you want recorded in the **Maximum number of log entries** field. A value of 0 means there is no limit.
4. Click **Update**.

Disabling the change log

To disable the change log:

1. In the Configuration Tool, click **Configure/unconfigure changelog** in the task list on the left.

2. In the Configure/unconfigure changelog window, clear the **Enable change log database** check box.
3. Click **Update**.

Managing suffixes

A suffix (also known as a naming context) is a distinguished name (DN) that identifies the top entry in a locally held directory hierarchy. Because of the relative naming scheme used in LDAP, this DN is also the suffix of every other entry within that directory hierarchy. A directory server can have multiple suffixes, each identifying a locally held directory hierarchy; for example, o=ibm,c=us.

Note: The specific entry that matches the suffix must be added to the directory.

Entries to be added to the directory must have a suffix that matches the DN value, such as ou=Marketing,o=ibm,c=us. If a query contains a suffix that does not match any suffix configured for the local database, the query is referred to the LDAP server that is identified by the default referral. If no LDAP default referral is specified, an **Object does not exist** result is returned.

Adding a suffix

To add a suffix:

1. In the Configuration Tool, click **Manage suffixes** in the task list on the left.
2. In the Manage suffixes window, type the suffix you want to add in the **SuffixDN** field, and click **Add**.
3. When you have added all the suffixes you want, click **OK**.

   Note: When you click **Add**, the suffix is added to the list in the **Current suffix DNs** box; however, the suffix is not actually added until you click **OK**.

Removing a suffix

To remove a suffix:

1. In the Configuration Tool, click **Manage suffixes** in the task list on the left.
2. In the Manage suffixes window, click the suffix you want to remove in the **Current suffix DNs** box, and click **Remove**.
3. When you have selected all the suffixes you want to remove, click **OK**.

   Notes:

   a. System files cannot be deleted.
   b. When you click **Remove**, the suffix is removed from the list in the **Current suffix DNs** box; however, the suffix is not actually removed until you click **OK**.

Managing schema files

You can use the Configuration Tool for the following schema file tasks:

- Adding a schema file to the list of schema files that will be loaded at startup
- Removing a schema file from the list of schema files that will be loaded at startup
- Changing the type of validation checking that is done for schema files

Adding a schema file

To add a schema file to the list of schema files that will be loaded at startup:

1. In the Configuration Tool, click **Manage schema files** in the task list on the left.

2. In the Manage schema files window, type the path and file name of the schema file you want to load at startup. (Alternatively, click **Browse** to search for the file.)
3. Click **Add**.

   Note: When you click **Add**, the schema file is added to the list in the **Current Schema Files** box; however, the schema file is not actually added until you click **OK**.
4. When you have added all the schema files you want, click **OK**.

Removing a schema file

To remove a schema file from the list of schema files that will be loaded at startup:

1. In the Configuration Tool, click **Manage schema files** in the task list on the left.
2. In the Manage schema files window, click the schema file you want to remove in the **Current Schema Files** box.
3. Click **Remove**.

   Notes:

   a. A schema file that contains the string `system` is a system file and cannot be deleted.

   b. When you click **Remove**, the schema file is removed from the list in the **Current Schema Files** box; however, the schema file is not actually removed until you click **OK**.
4. When you have selected all the schema files you want to remove, click **OK** to process the files.

Changing the type of validation checking that is done

To change the type of validation checking that is done on schema files:

1. In the Configuration Tool, click **Manage schema files** in the task list on the left.
2. In the Manage schema files window, accept the default schema validation rule in the **Schema Validation Rules** box, or click the rule you want. You can select one of the following:
   - Version 3 (Strict)

     LDAP version 3 strict validation checking is done. With this type of validation checking, all parent object classes must be present when adding entries.
   - Version 3 (Lenient)

     LDAP version 3 lenient validation checking is done. With this type of validation checking, all parent object classes do not need to be present when adding entries.

     This is the default.
   - Version 2

     LDAP version 2 checking is done.
   - None

     No validation checking is done.
3. Click **OK**.

Importing and exporting LDIF data

You can use the Configuration Tool to import data from an LDAP Data Interchange Format (LDIF) file or to export data from the database to an LDIF file. LDIF is used to represent LDAP entries in text form. When importing, you can add entries

to an empty directory database or to a database that already contains entries. You can also use the Configuration Tool to validate the data in the LDIF file without adding the data to the directory.

Importing LDIF data

Note: Before you import the data from an LDIF file, be sure to add any necessary suffixes. See "Adding a suffix" on page 68 for information about adding a suffix.

To import data from an LDIF file:

1. In the Configuration Tool, click **Import LDIF data** in the task list on the left.
2. In the Import LDIF data window on the right, type the path and file name of the LDIF file in the **Path and LDIF file name** field. Alternatively, you can click **Browse** to locate the file.
3. Click **Standard import** if you want to import the data using the **ldif2db** utility, or click **Bulkload** if you want to import the data using the **bulkload** utility.

   Note: For large LDIF files, the **bulkload** utility is a faster alternative to **ldif2db** if you are importing a large number of entries.
4. If you clicked **Bulkload**, click the type or types of checking you want to perform on the LDIF data in the **Bulkload Options** box. You can select one or more of the following:
   - Enable schema checking
   - Enable ACL checking
   - Enable password policy

   Click **Import**.

Validating LDIF data without adding it to the database

To validate the data in the LDIF file without adding it to the database:

1. In the Configuration Tool, click **Import LDIF data** in the task list on the left.
2. In the Import LDIF data window on the right, type the path and file name of the LDIF file in the **Path and LDIF file name** field. Alternatively, you can click **Browse** to locate the file.
3. Click **Data Validation only**.
4. Click **Import**.

Exporting LDIF data

To export data from the database to an LDIF file:

1. In the Configuration Tool, click **Export LDIF data** in the task list on the left.
2. In the Export LDIF data window on the right, type the path and file name of the LDIF file in the **Path and LDIF file name** field. Alternatively, you can click **Browse** to locate the file.
3. If you want to overwrite the data in an existing file, select the **Overwrite if file exists** check box.
4. If you want to export only some of the data in the directory, complete the **Subtree DN** field. The subtree DN identifies the top entry of the subtree that is to be written to the LDIF output file. This entry, plus all entries below it in the directory hierarchy, are written to the file. If you do not specify this option, all directory entries stored in the database are written to the output file based on the suffixes specified in the IBM Directory Server configuration file.
5. Click **Export**.

Backing up, restoring, and optimizing the database

You can use the Configuration Tool for the following database tasks:

- Backing up the data in the database
- Restoring data and, optionally, configuration settings that were previously backed up
- Updating statistics related to the data tables for the purpose of improving performance and query speed

Backing up the database

The directory server must be stopped before you can back up the database.

To back up the database:

1. In the Configuration Tool, click **Backup database** in the task list on the left.
2. In the Backup database window on the right, in the **Backup directory** field, type the directory path in which to back up all directory data and configuration settings. Alternatively, click **Browse** to locate the directory path.
3. Click one of the following:
   - **Create backup directory as needed** if you want the directory to be created if it does not exist.
   - **Abort if backup directory is not found** if you do not want the directory you specified to be created. If this directory does not exist and you select this option, the database will not be backed up.
4. Click **Backup**.

Restoring the database

To restore the database:

1. In the Configuration Tool, click **Restore database** in the task list on the left.
2. In the Restore database window on the right, in the **Backup directory** field, type the path in which the directory was previously backed up. Alternatively, click **Browse** to locate the path.
3. If you want to restore only the directory data, but not the configuration settings, Select the **Restore data only (not configuration settings)** check box. If you want to restore both data and configuration settings, be sure the check box is cleared.
4. Click **Restore**.

Optimizing the database

Optimize the database to update statistics related to the data tables; this can improve performance and query speed. Perform this action periodically or after heavy database updates; for example, after importing database entries.

1. In the Configuration Tool, click **Optimize database** in the task list on the left.
2. In the Optimize database window on the right, click **Optimize**.

Using the ldapcfg utility

The ldapcfg utility is a command-line tool that you can use to configure the IBM Directory Server. You can use ldapcfg instead of the Configuration Tool for the following tasks:

- Setting the administrator DN and password. See “Setting the administrator DN and password” on page 72 for instructions.
- Configuring a database. See “Configuring the database” on page 72 for instructions.

- Enabling the change log. See "Enabling the change log" on page 73 for instructions.
- Adding a suffix. See "Adding a suffix" on page 73 for instructions.

Setting the administrator DN and password

To define the administrator DN and password, type the following at a command prompt:

```
ldapcfg -u "adminDN" -p password
```

where

- *adminDN* is the administrator DN you want.
- *password* is the password for the administrator DN.

For example:

```
ldapcfg -u "cn=root" -p secret
```

Note: Do not use single quotation marks (') to define DNs with spaces in them. They are not interpreted correctly.

To accept the default administrator DN of cn=root and define a password, type the following command at a command prompt:

```
ldapcfg -p password
```

where *password* is the password for the administrator DN.

For example:

```
ldapcfg -p secret
```

Configuring the database

When you configure the database, you must always specify a user ID and password on the command line. The instance name is no longer required (or allowed) since it must be the same as the user name. The user ID must already exist and must meet certain requirements. See "Before you configure: creating the DB2 database owner" on page 65 for information about these requirements on both Windows and UNIX platforms.

Notes:

1. Before configuring the database, be sure that the environment variable DB2COMM is **not** set.
2. Be sure to read this section before you use the **ldapcfg** command. Some options (such as **-f** and **-s**) have changed. Unpredictable results will occur if you use them incorrectly or as they were used in previous releases.

To configure a database, the following options are available:

-l *location*
: Location of the DB2 database. For UNIX systems, this is a directory name such as /home/ldapdb. For Windows systems, this is a drive letter such as c:.

-a *id*
: DB2 administrator ID.

-c
: Create a database in UTF-8 format. (The default, if you do not specify this option, is to create a database that is in the local code page.)

-i Destroy any instance currently configured with the IBM Directory Server. All databases associated with the instance are also destroyed.

-w *password*
DB2 administrator password.

Note: The **ldapcfg -w** *password* command no longer changes the system password of the database owner. It only updates the ibmslapd.conf file.

-d *database*
DB2 database name.

-o Overwrite the database if one already exists. By default, the database being overwritten is not deleted.

-r Destroy any database currently configured with the IBM Directory Server.

-f Full path of a file to redirect output into. If used in conjunction with the **-q** option, only errors will be sent to the file.

-q Run in quiet mode. All output is suppressed except for errors.

-n Run in no prompt mode. All output is generated except for messages requiring user interaction.

To configure a database on /home/ldapdb2 with a DB2 administrator name of **db2admin**, a password of **mypassword**, and a database name of **dbName** when there is not an existing database configured (that is, the first time), the command is:

```
ldapcfg -l /home/ldapdb2 -a db2admin -w mypassword -d dbName
```

To configure a database on /home/ldapdb2 when a database is already configured and you want to overwrite it, the command is:

```
ldapcfg -l /home/ldapdb2 -a db2admin -w mypassword -d dbName -o
```

For information about unconfiguring a database using the **ldapucfg** command-line utility, see "Unconfiguring the server" on page 77.

Enabling the change log

To enable the change log use the **-g** option. The change log is a separate database that records changes to the main directory. You need an additional 30 MB to create it.

To set the maximum number of entries that will be logged in the change log, use the **-m** *maxentries* option. If you do not specify a maximum number, the default of 0 means there is no limit to the number of entries.

For information about disabling the change log using the ldapucfg command-line utility, see "Unconfiguring the server" on page 77.

Adding a suffix

To add suffixes to the ibmslapd.conf file using the **ldapcfg** utility, the command is:

```
ldapcfg -s "suffix"
```

where *suffix* is the suffix you want to add.

Importing or exporting data

To import data from an LDIF file, you can use either the **ldif2db** or the **bulkload** utility.

To export data to an LDIF file, you can use the **db2ldif** utility.

See the *IBM Directory Server version 5.1 Administration Guide* for instructions.

Backing up, restoring, and optimizing the database

The following sections describe how to back up, restore, and optimize the database using command line utilities.

Backing up the database using the dbback command

To back up the directory database using the command line, use the **dbback** utility.

Note: This utility uses the ibmslapd.conf configuration file.

The following options are available:

-d *directory*
The directory in which you want to back up the database. The user ID that owns the configured directory database must have write access to this directory.

-w *filename*
The full path and file name of a file into which you want to redirect output.

Restoring the database using the dbrestore command

To restore the directory database using the command line, use the **dbrestore** utility.

The following options are available:

-d *directory*
The directory from which to restore the database.

-n Specifies not to restore the ibmslapd.conf file.

-w *filename*
The full path and file name of a file into which you want to redirect output.

Optimizing the database using the runstats command

To optimize the directory database using the command line, use the **runstats** command. This command updates statistics related to the data tables.

The following option is available:

-f *config_file_name*
The name of the configuration file. If not specified, ibmslapd.conf is used.

Chapter 11. After you install and configure

After you install the server, set the administrator DN and password, and configure the database, you can start the directory server. If you installed the Web Administration Tool and the embedded version of WebSphere Application Server - Express, V5.0, you can start the application server.

Starting the directory server

To start the directory server, type `ibmslapd` at a command prompt.

For information about performing administrative tasks using the Web Administration Tool and the command line, see the *IBM Directory Server version 5.1 Administration Guide*.

For information about stopping the server, see the *IBM Directory Server version 5.1 Administration Guide*.

Starting the application server to use the Web Administration Tool

If you are using embedded version of WebSphere Application Server - Express, V5.0 as your application server, go to the directory where you installed the embedded version of WebSphere Application Server - Express, V5.0 and type `startServer server1` at a command prompt.

For information about stopping the application server and about using the Web Administration Tool, see the *IBM Directory Server version 5.1 Administration Guide*.

Starting the Web Administration Tool

To start the Web Administration Tool:

1. After you have started the application server, from a Web browser, type the following address: http://localhost:9080/IDSWebApp/IDSjsp/Login.jsp

   The IBM Directory Server Web Administration login page window is displayed.

   Note: This address works only if you are running the browser on the computer on which the Web Administration Tool is installed. If the Web Administration Tool is installed on a different computer, replace **localhost** with the hostname of the computer where the Web Administration Tool is installed.

   For information about using the Web Administration Tool, see the *IBM Directory Server version 5.1 Administration Guide*.

Chapter 12. Unconfiguring the server and uninstalling IBM Directory Server

To remove the IBM Directory Server from your computer, you must first unconfigure, and then uninstall, the server. Use the sections in this chapter to unconfigure and remove.

Unconfiguring the server

The options for the **ldapucfg** utility are similar to the **ldapcfg** utility except that in the **ldapucfg** utility:

- The **-d** option removes the currently configured DB2 database. It also removes the change log if enabled.
  - The **-r** option, used with **-d**, destroys any database currently configured with the IBM Directory Server without prompting for information.
  - The **-i** option, used with **-d**, destroys any instance currently configured with the IBM Directory Server without prompting for information. All databases associated with the instance are destroyed also.
- The **-g** option disables the change log. Disabling the change log removes the change log database and any data (change records) that are in it. The **-g** option does not affect the main directory database.

Note: If you are unconfiguring a UNIX-based system, you must run **ldapucfg**) from a directory that has execute permission for **other**. That is, the directory must have at least the **--------x** permission set. If this permission is not set, you might see an error message and experience a subsequent failure. To set this permission for your current directory, you can enter the command:

```
chmod o+x .
```

The period (.) in the command is required to indicate the current directory.

Attention: Back up any existing schema files and your directory before performing the following steps.

To remove the DB2 configuration information:

1. On UNIX platforms, log in as **root**. On Windows systems, log on as an administrator.
2. Stop all clients that are connected to the IBM Directory Server server.
3. Use the **ldapucfg** utility to remove the DB2 configuration information from the server. At the command prompt, enter:

   ```
   ldapucfg -d
   ```

   You might be prompted for more information about removing the database and the DB2 instance.

Uninstalling IBM Directory Server

After you unconfigure, use the following sections to uninstall IBM Directory Server.

Uninstalling using operating system utilities

After you remove the configuration information, you can uninstall the IBM Directory Server.

Notes:

1. If you installed IBM Directory Server using the InstallShield GUI, uninstall using the process in "Uninstalling using the InstallShield GUI" on page 80.
2. Removing the IBM Directory Server does not remove any databases you created using IBM Directory Server.

AIX operating system

To uninstall the IBM Directory Server server or client, type the following:

```
installp -u ldap
```

This removes only IBM Directory Server filesets. It does not remove other components such as DB2.

HP-UX

To remove the IBM Directory Server, complete the following steps:

1. At a command prompt, type `swremove`
2. Select the installed IBM Directory Server.
3. Click **Actions-->Mark For Remove**.
4. Click **Actions-->Remove/Uninstall**.
5. Click **OK**.
6. When removal is complete, click **Done**.
7. Click **File-->Exit**.

Linux operating system

Before removing the IBM Directory Server, ensure that the server is stopped and then issue the following commands.

Note: If the IBM Directory Server server is installed, you must remove the server before you remove the client (the reverse order of the installation).

```
rpm -ev ldap-server-5.1-1
rpm -ev ldap-webadmin-5.1-1
rpm -ev ldap-client-5.1-1
rpm -ev ldap-msg-xxx-5.1-1.i386.rpm (Where xxx is
language dependent.)
rpm -ev ldap-html-xxx-5.1-1.i386.rpm (Where xxx is
language dependent.)
```

Solaris operating system

You can uninstall the IBM Directory Server using the **admintool** utility or from a command line using **pkgrm**.

AdminTool Removal: To remove the IBM Directory Server using the admintool utility:

1. Log in as **root**.
2. Type the following at a command prompt:

   ```
   admintool&
   ```

   The **Users** window is displayed.
3. Click **Browse -> Software**. The **Software** window is displayed.

4. Select the packages to delete from the displayed list.

   ```
   IBM Directory Client
   IBM Directory Documentation
   IBM Directory Messages
   IBM Directory Server
   IBM Directory Webadmin
   ```

5. Click **Edit ->Delete**. The **AdminTool: Warning** window is displayed.
6. Click **Delete**.

   Note: With the removal of client and server packages, the system prompts you with the query, `This package contains scripts which will be executed with super-user permission during the process of installing the package. Continue with the removal of this package?` Type `y` to continue. If you are removing the Server package, you also see the prompt, `Do you want to remove these as setuid and/or setgid files?`Type `y` to continue.
7. After the package is removed, the **Software** window is displayed. When the removal is complete, type `q` to return to the command prompt.

Installing the IBM Directory Server using the default settings creates the opt/IBMldaps and opt/IBMldapc directories. If you uninstall the IBM Directory Server, the removal procedure might not remove these directories. If one or both of these directories exist, they create a problem if you later reinstall the IBM Directory Server in non-default directories.

To ensure that the directories are completely removed issue this command at a command line:

```
rm -fr /opt/IBMldaps /opt/IBMldapc
```

You can now reinstall the IBM Directory Server to a non-default directory.

Note: This problem does not occur if you reinstall to the default directories.

Command Line Removal: To see what IBM Directory Server components are installed, type:

```
pkinfo | grep -i ibml
```

The output displayed is similar to the following:

```
IBMldapc    IBM Directory Client
(sparc) 5.1.0.0
IBMldaps     IBM Directory Server
      (sparc) 5.1.0.0
IBMldixxx    IBM Directory documentation
 (sparc) 5.1.0.0
IBMldmxxx    IBM Directory messages
(sparc) 5.1.0.0
IBMldapw                        IBM Directory Webadmin
(sparc) 5.1.0.0
```

Use **pkgrm** to remove the desired packages. For example:

```
pkgrm IBMldaps IBMldapc IBMldapw
```

You can specify either the package name or its listing number. Remove the packages in the reverse order of the installation sequence. (The order in which you remove the Web Administration Tool is not important.)

Uninstalling using the InstallShield GUI

The following sections describe how to uninstall the IBM Directory Server using the InstallShield GUI.

Windows platforms

To remove IBM Directory Server on a Windows platform using the InstallShield GUI:

1. Click **Start-->Settings-->Control Panel-->Add/Remove Programs**.
2. Select **IBM Directory Server 5.1**. Click **Change/Remove**.
3. Select the language you want to use during the uninstall. Click **OK**.
4. On the Welcome window, click **Next**.
5. Select the features you want to uninstall. Click **Next**.
6. On the confirmation window, to uninstall the selected features, click **Next**.

UNIX platforms

To remove IBM Directory Server on a UNIX platform using the InstallShield GUI:

1. At a command prompt, go to the IBM Directory Server `_uninst` directory.
   - On AIX and Linux operating systems, this directory is/usr/ldap/_uninst.
   - On the Solaris operating system, this directory is /opt/IBMldapc/_uninst.
2. Run the uninstall command:

   ```
   ./uninstall
   ```
3. Select the language you want to use during the uninstall. Click **OK**.
4. On the Welcome window, click **Next**.
5. Select the features you want to uninstall. Click **Next**.
6. On the confirmation window, to uninstall the selected features, click **Next**.

Chapter 13. Troubleshooting

If you are having problems installing or configuring IBM Directory Server 5.1, refer to this section for possible fixes.

InstallShield GUI installation

If installation does not complete, the first place you can look for information is the ldapinst.log file. If the installation destination directory (*install directory*) was created, this log is in the *install directory* root directory. For example, on a Windows system, the ldapinst.log file is, by default, in c:\Program Files\IBM\LDAP\. If *install directory* was not created before the installation failed, the log might be in a temporary directory. To find it, search for "ldapinst.log". Review this log for any messages about why the installation failed. Because some of the LDAP features require corequisite products, it is possible that a failure in a corequisite installation caused the IBM Directory Server installation to fail. For example, if the server feature is being installed, but the DB2 installation fails, the server feature cannot be installed.

Logs used by the InstallShield GUI when installing embedded version of WebSphere Application Server - Express, V5.0 are:

On Windows platforms

- Documents and Settings*userid*\Local Settings\Temp\installApp.log
- Documents and Settings*userid*\Local Settings\Temp\installAppErr.log
- Documents and Settings*userid*\Local Settings\Temp\configApp.log
- Documents and Settings*userid*\Local Settings\Temp\configAppErr.log

On UNIX platforms

- /tmp/installApp.log
- /tmp/installAppErr.log
- /tmp/configApp.log
- /tmp/configAppErr.log

Logs used by the InstallShield GUI when installing and uninstalling DB2 on Windows are:

When installing

- Documents and Settings*userid*\Local Settings\Temp\DB2setup.log
- Documents and Settings*userid*\Local Settings\Temp\db2wi.log
- Documents and Settings*userid*\Local Settings\Temp\db2inst.log
- Documents and Settings*userid*\Local Settings\Temp\db2insterr.log

When uninstalling

- Documents and Settings*userid*\Local Settings\Temp\DB2remove.log
- Documents and Settings*userid*\Local Settings\Temp\db2uninst.log
- Documents and Settings*userid*\Local Settings\Temp\db2uninsterr.log
- Documents and Settings*userid*\Local Settings\Temp\db2uninsttrc.log

Failed installation

Another reason for failed installation is lack of disk space. IBM Directory Server attempts to verify that there is enough space and generates messages if the requisite disk space is not found, but it is possible that InstallShield GUI cannot progress far enough to issue a message. Before installing, make sure you have the recommended free disk space. All platforms use temporary space, and in addition, UNIX platforms use the `/var` directory. When install is first executed, the JVM is installed to the installation directory, so be sure that your installation destination directory has enough space.

Recovering from a failed installation

The first step to recovering from a failed installation is to run the InstallShield Uninstall GUI to clean up any registry entries that might have been made by the install. If you do not run the InstallShield Uninstall GUI, the InstallShield GUI might fail the next time you try to install using the InstallShield GUI. See the following sections for information about how to do this for each platform. See "Uninstalling using the InstallShield GUI" on page 80 for information about uninstalling using the InstallShield GUI.

When installing on UNIX platforms, the IBM Directory Server InstallShield GUI uses the native packages (i.e. AIX installp files, Solaris .pkg files, or RPM files) to install. Because of this, you will see these packages when you run the platform commands (such as rpm -qa on Linux operating system) to query what is installed. Even though you can use the platform commands (such as rpm -e) to uninstall, you **must** use the InstallShield GUI to uninstall so that the InstallShield Registry is cleaned up.

AIX operating system

On the AIX operating system:

1. Uninstall using the InstallShield GUI.
2. Type the following at a command prompt:

   ```
   lslpp -L |grep -i ldap
   ```
3. If any packages that were installed by IBM Directory Server were left on the system, use **installp** to uninstall them, as follows:

   ```
   installp -u package name
   ```
4. Remove the /usr/ldap directory.
5. Correct any other problems that were listed in the ldapinst.log.

   Note: AIX operating system installation will generate an additional log called installp_isje.log. You must review this log to determine if there were failures in the **installp** commands issued by the InstallShield GUI.

Linux operating system

On the Linux operating system:

1. Uninstall using the InstallShield GUI.
2. Type the following at a command prompt:

   ```
   rpm -qa | grep -i ldap
   ```

   If any packages that were installed by IBM Directory Server were left on the system, use the **rpm** command to uninstall them. For example:

   ```
   rpm -ev  package names
   ```
3. If an rpm command hangs, try running the command with the noscripts options:

```
rpm -ev  --noscripts package names
```

4. Remove the /usr/ldap directory
5. Correct any other problems that were listed in the ldapinst.log.

Solaris operating system

On the Solaris operating system:

1. Uninstall using the InstallShield GUI.
2. Type the following at a command prompt:
   ```
   pkginfo | grep -i ldap
   ```
3. If any packages that were installed by IBM Directory Server were left on the system, use **pkgrm** to uninstall them:
   ```
   pkgrm package names
   ```

   Note: If you encounter problems removing these packages, try to remove the directories containing the packages from /var/sadm/pkg
4. Remove the /opt/IBMldapc and /opt/IBMldaps directories, and any other directories left from the install, such as a language directory.
5. Correct any other problems that were listed in the ldapinst.log.

Windows operating system

On Windows:

1. Uninstall using the InstallShield GUI.
2. Remove the IBM Directory Server installation directory. The default directory is C:\Program Files\IBM\LDAP.
3. Correct any other problems listed in the ldapinst.log file.
4. Use **regedit** to remove the LDAP entry in the registry: HKEY_LOCAL_MACHINE\SOFTWARE\IBM\LDAP
5. Remove the following environment variables:

   LANG=enus1252
   LDAPHome=C:\Program Files\IBM\LDAP
   LIBPATH=C:\Program Files\IBM\LDAP\JAVA
   LOCPATH=C:\Program Files\IBM\LDAP\bin\locale
   NLSPATH=C:\Program Files\IBM\LDAP\NLS\MSG\%L\%N
   Path=C:\ProgramFiles\IBM\LDAP\bin
   TISDIR=C:\Program Files\IBM\LDAP

Configuration

If you see the following message during the configuration of the database

```
Failed to start database manager for instance: ldapdb2
```

you might have a problem with your electronic DB2 license. To verify this, type the following at the command prompt:

```
db2start
```

If your license is correct, you see the message:

```
SQL1063N DB2START processing was successful.
```

Otherwise, you see a message indicating that your license has expired.

If there is a problem with your electronic DB2 license, one of the following situations might be the cause:

- You have a demonstration license.
  1. To upgrade your DB2 product from a demonstration license to a product license, copy the license file from the DB2 CD to the system where DB2 is installed; you do not need to reinstall the product.

     Note: Your Proof of Entitlement and License Information booklets identify the products for which you are licensed.
  2. After you have a valid license on the system, run the following command to activate the license:

     ```
     db2licm -a db2udbee.lic
     ```
- You have purchased a different DB2 product.

  If you install a DB2 product as Try-and-Buy, and you buy a different DB2 product, you must uninstall the Try-and-Buy product and then install the new one that you have purchased. Type the following at a command prompt to upgrade your DB2 license:

  ```
  db2licm -a db2udbee.lic
  ```

DB2 does not configure properly

Note: Before configuring the database, be sure that the environment variable DB2COMM is **not** set.

If a failure occurs during database configuration, usually one of the following is the cause:

- The user ID was not set up correctly. See "Before you configure: creating the DB2 database owner" on page 65 for information.
- The permissions for the user ID are not correct. See "Before you configure: creating the DB2 database owner" on page 65 for information.
- Remnants of a previous database or DB2 instance with the name you specified for the database are present on the system.
- There is not enough space in the location you specified.

Check to see if there are problems with any of these items, and then try to configure again after you fix the problem.

Note: If you use the Configuration Tool to configure and configuration fails, the Configuration Tool does some cleanup, and this can sometimes fix the problem. If you do not find any of the problems in the list, try configuring again.

Database performance is poor

The BUFFPAGE and DBHEAP database configuration parameters can affect performance. The default BUFFPAGE included with DB2 is 1000 (4 KB pages), which might not be big enough for a large database. Also, if you increase the BUFFPAGE parameter, you must also increase the DBHEAP size by 1 for every 30 incremented in the BUFFPAGE.

DB2 database supports multiple buffer pools. However, unless you know how to do specialized tuning on DB2, it is recommended that you use a single buffer pool. This can be specified using the command:

```
db2 alter bufferpool ibmdefaultbp size -1
```

To update the database configuration parameters for a database, use the command:

```
db2 update database configuration for databasename using
       param value
```

For example, to increase the BUFFPAGE and DBHEAP size, use the command:

```
db2 update database configuration for databasename using
       BUFFPAGE 20000 DBHEAP 1866
```

Note: For more detailed performance information, see the *IBM Directory Server Version 5.1 Tuning Guide*.

Referral fails on Linux, Solaris, or HP-UX

On the Linux, Solaris, and HP-UX platforms, if a referral fails, ensure that the environment variable LDAP_LOCK_REC has been set in your system environment. No specific value is required.

```
set LDAP_LOCK_REC=anyvalue
```

Transaction log is full

The following messages might be displayed at IBM Directory Server startup if the schema defines too many attributes:

```
SQL0965C The transaction log for the database is full
SQLSTATE=57011 slapd unable to start because all backends failed to configure
```

You might need to increase the DB2 transaction log sizes by typing:

```
db2 update db cfg for ldaptest using logprimary X
db2 update db cfg for ldaptest using logsecond X
```

where X is greater than what is currently defined.

Debugging

The following sections provide debugging information.

DB2 Errors Logged

In addition to the ibmslapd.log file, which can be accessed through the Web Administration Tool, DB2 errors are logged in the db2cli.log file. Both files are located in the var subdirectory of the IBM Directory Server installation directory on Windows platforms.

Note: The var subdirectory might include other DB2 files.

Server errors are logged in the \var\ibmslapd.log file.

DB2 errors are logged in the \var\db2cli.log file.

Server Debug Mode

If the error logs do not provide enough information to resolve a problem, you can run the server in a special debug mode that generates very detailed information. The server executable ibmslapd must be run from a command prompt to enable debug output. The syntax is as follows:

```
ldtrc on
ibmslapd -h bitmask
```

where the specified bitmask value determines which categories of debug output are generated.

For example, the following ldtrc search:

```
ldapsearch -l 60 -h ddejesus -D "o=IBM_US, c=US" -w
secret -b "ou=Austin, o=IBM_US, c=US" "cn=Cindy Corn"
```

might return server output similar to the following:

```
Connection received from 9.53.95.251 on socket 540.
  86366975        704 usec SQLAllocStmt() => 0
  86367557         73 usec SQLBindParameter() => 0
  86367974         33 usec SQLBindParameter() => 0
  86435508         52 usec SQLFetch => 0
  86436039         49 usec SQLGetData => 0
  86436835        454 usec SQLFreeStmt => 0
  86458726        629 usec SQLAllocStmt() => 0
  86459708        561 usec SQLPrepare(SELECT distinct
DB2ADMIN.LDAP_ENTRY.EID FROM DB2ADMIN.LDA
P_ENTRY,DB2ADMIN.LDAP_DESC  WHERE
(DB2ADMIN.LDAP_ENTRY.EID=DB2ADMIN.LDAP_DESC.DEID
AND DB2ADMIN.LDAP_DESC.AEID=?) AND  DB2ADMIN.LDAP_ENTRY.EID
IN (SELECT EID FROM DB2ADMIN.CN WHERE CN_T= ?)) => 0
```

See Table 2 for a description of debug categories.

Table 2. Debug categories

Hex	Decimal	Value	Description
0x0001	1	LDAP_DEBUG_TRACE	Entry and exit from routines
0x0002	2	LDAP_DEBUG_PACKETS	Packet activity
0x0004	4	LDAP_DEBUG_ARGS	Data arguments from requests
0x0008	8	LDAP_DEBUG_CONNS	Connection activity
0x0010	16	LDAP_DEBUG_BER	Encoding and decoding of data
0x0020	32	LDAP_DEBUG_FILTER	Search filters
0x0040	64	LDAP_DEBUG_MESSAGE	Messaging subsystem activities and events
0x0080	128	LDAP_DEBUG_ACL	Access Control List activities
0x0100	256	LDAP_DEBUG_STATS	Operational statistics
0x0200	512	LDAP_DEBUG_THREAD	Threading statistics
0x0400	1024	LDAP_DEBUG_REPL	Replication statistics
0x0800	2048	LDAP_DEBUG_PARSE	Parsing activities
0x1000	4096	LDAP_DEBUG_PERFORMANCE	Relational backend performance statistics
0x1000	8192	LDAP_DEBUG_RDBM	Relational backend activities (RDBM)
0x4000	16384	LDAP_DEBUG_REFERRAL	Referral activities
0x8000	32768	LDAP_DEBUG_ERROR	Error conditions
0xffff	65535	ALL	
0x7fffffff	2147483647	LDAP_DEBUG_ANY	All levels of debug

For example, specifying a bitmask value of 65535 turns on full debug output and generates the most complete information.

When you are finished, issue the following command at a command prompt:

```
ldtrc off
```

It is recommended that you contact IBM Service for assistance with interpreting the debug output and resolving the problem.

Migration

During migration, the following log files might be created.

On UNIX platforms:

Errors that occurred during schema migration are logged in the /tmp/migrate.errors file.

Detailed messages concerning schema migration are logged in the /tmp/migrate51.log file.

On Windows platforms:

Migration errors are logged in the *install directory*\tmp\migrate51.err file.

Migration information messages are logged in the *install directory*\tmp\migrate51.out file.

Web browser problems

The following information might be helpful if you encounter problems with your Web browser.

Microsoft Internet Explorer

Cache Setup

Click **View->Internet Options** , and select **General**. Then, click **Settings**. Under **Check for newer versions of stored pages**, click **Every visit to the page**.

If you are getting unpredictable results using the browser, the cache might be storing pages with errors. On the General folder page, click **Delete files** and **Clear History** to clear the cache. Use these options as often as necessary.

Shutting down and restarting the browser can also repair some intermittent problems.

Netscape

Cache Setup

Click **Edit->Preferences->Advanced->Cache**. Under **Document in cache is compared to document on network**, click **Every time**.

On this same page, if you are getting unpredictable results using the browser, click **Clear Memory Cache** and **Clear Disk Cache** to clear the cache. You can use these buttons as often as necessary.

Shutting down and restarting the browser can also improve some intermittent problems.

Appendix A. Database configuration planning

Before configuring and populating your database, determine:

What type of data you are going to store in the directory
Decide what sort of schema you need to support the type of data you want to keep in your directory. A standard set of attribute-type definitions and object-class definitions are included with the directory server. Before you begin adding entries to the directory, you might want to add new attribute-type and object-class definitions that are customized to your data.

Note: You can make schema additions after the directory is already populated with data, but schema changes might require you to unload and reload your data.

Which code page you are going to use
Decide whether to create your database using the local code page or using the Universal Character Set (UTF-8). Selecting the local code page enables IBM Directory Server applications and users to get search results as expected for the collation sequence of the native language. Using UTF-8 enables the storing of any UTF-8 character data in the directory. IBM Directory Server clients running anywhere in the world (in any UTF-8 supported language) can access and search the directory. In many cases, however, the client might have limited ability to properly display the results retrieved from the directory in a particular language or character set. See Appendix F, "UTF-8 support" on page 101 for more information.

How you want to structure your directory data
An IBM Directory is stored in a hierarchical tree structure. The names of entries in the directory are based on their relative position within the tree structure. It is important to define some logical organization to the directory. This makes it easier for clients to determine which branch of the tree contains the information they are trying to locate. If you are storing data about the people in an organization, it is easy to map the structure of the organization onto the structure of the directory. If you are storing descriptions of applications, machine configuration data, or data on customers, it might take more planning to decide how to structure your directory.

Your data security requirements
See the Secure Sockets Layer information in the *IBM Directory Server version 5.1 Administration Guide* for information about how your data is secured.

How you want to allocate access permissions
See the Access Control Lists information in the *IBM Directory Server version 5.1 Administration Guide* for information about using access permissions.

Return to Chapter 1, "Installation, configuration, and migration overview" on page 1 or to Chapter 10, "Configuration" on page 63.

Appendix B. Support for additional locales on UNIX platforms

On some UNIX systems, depending on your locale settings, server messages might be generated in English, rather than in the language associated with the locale. For example, if your locale is set to de_DE, then German messages are displayed. However, if you locale is set to de_CH, then English messages are displayed.

If this occurs, you can create symbolic links to select a language for messages on AIX, Linux, or HP-UX.

For example, on AIX or Linux, to select German messages for a locale in Switzerland, (de_CH), create links by typing the following at a command prompt:

```
cd /usr/lib/nls/msg
ln -sf de_DE/diradm.cat de_CH/diradm.cat
ln -sf de_DE/ldapc.cat de_Ch/ldapc.cat
ln -sf de_DE/ldapcp.cat de_Ch/ldapcp.cat
ln -sf de_DE/ldapprod.cat de_Ch/ldapprod.cat
ln -sf de_DE/ldaputil.cat de_Ch/ldaputil.cat
ln -sf de_DE/ldcf.cat de_Ch/ldcf.cat
ln -sf de_DE/rdbm.cat de_Ch/rdbm.cat
ln -sf de_DE/slapd.cat de_Ch/slapd.cat
ln -sf de_DE/webutil.cat de_Ch/webutil.cat
```

On HP-UX, for example, to enable the Spanish translation for a locale in Mexico, (es_MX), create links by typing the following at a command prompt:

```
cd /usr/lib/nls/msg
ln -sf es_ES.iso88591/diradm.cat es_MX.iso88591/diradm.cat
ln -sf es_ES.iso88591/ldapc.cat es_MX.iso88591/ldapc.cat
ln -sf es_ES.iso88591/ldapcp.cat es_MX.iso88591/ldapcp.cat
ln -sf es_ES.iso88591/ldapprod.cat es_MX.iso88591/ldapprod.cat
ln -sf es_ES.iso88591/ldaputil.cat es_MX.iso88591/ldaputil.cat
ln -sf es_ES.iso88591/ldcf.cat es_MX.iso88591/ldcf.cat
ln -sf es_ES.iso88591/rdbm.cat es_MX.iso88591/rdbm.cat
ln -sf es_ES.iso88591/slapd.cat es_MX.iso88591/slapd.cat
ln -sf es_ES.iso88591/webutil.cat es_MX.iso88591/webutil.cat
```

Appendix C. Migrating a network of replicating servers

Previous versions of the IBM Directory Server and the SecureWay Directory Server supported replication in two configurations: single master with multiple replicas and multiple peer-masters with multiple replicas. Both of these configurations can be migrated to use the new replication topology required in IBM Directory Server 5.1. See "Migrating a single master configuration" or "Migrating a peer-master configuration" on page 95 for instructions.

Migrating a single master configuration

To migrate a configuration using a single master, first migrate the master and replica servers. See Chapter 3, "Migration from previous releases" on page 17 for information about how to migrate a server. As the master is started the first time, it will migrate the information in the directory that controlled replication. The entries with objectclass replicaObject under cn=localhost will be replaced with entries used by the new replication model. Each of the suffixes (except for cn=localhost and cn=changelog) will be treated as replication contexts; that is, an auxiliary objectclass of ibm-replicationContext will be added. Under each suffix entry there will be a new entry with a relative DN ibm-replicaGroup=default. This entry will have a child with a relative DN containing the unique server ID for this server. This is the replica subentry. It is this entry that determines that this particular server is a master of the replicated subtree. The server ID must match the server ID set in the server's configuration file, which was assigned and saved as the server started. This entry is the parent for all of the replica agreement entries that were generated from the migrated replicaObjects. The replica agreement entries define a replication path from this master to each of its replicas. The agreement entries are created with the attribute ibm-replicationOnHold set to true. This allows updates made to the master to be accumulated for the replica until the replica is ready.

These entries are referred to as the replication topology. The new master can be used with replicas running prior versions; data related to the new features will not be replicated to the back-level servers. It is necessary to export the replication topology entries from the master and add them to each replica after the replica server has been migrated. To export the entries, use the command line tool **ldapsearch** and save the output to a file. The search command is similar to the following:

```
ldapsearch -h master-server-host-name -p master-server-port \
 -D master-server-admin-DN -w master-server-admin-password \
 -b ibm-replicagroup=default,suffix-entry-DN \
 -L "(|(objectclass=ibm-replicaSubEntry)(objectclass=ibm-replicationAgreement))" \
     > replication.topology.ldif
```

This command creates an output LDIF file named replication.topology.ldif in the current working directory. The file contains only the new entries.

Note: Do not include the following suffixes:

- cn=changelog
- cn=localhost
- cn=pwdpolicy
- cn=schema

- cn=configuration

  Include only user-created suffixes.

Repeat the command for each suffix entry on the master, but replace ">" with ">>" to append the data to the output file for subsequent searches. After the file is complete, copy it to the replica servers.

Add the file to the replica servers after they have been successfully migrated; do not add the file to servers running previous versions of the directory server. You must start and stop the server before you add the file. To start the server, type `ibmslapd` at a command prompt. To stop the server, type the following at a command prompt.

```
ibmdirctl -h hostname -D adminDN -w adminPW -p port stop
```

When you add the file to a replica server, be sure that the replica server is not started. To add the data, use the **Import LDIF data** option in the Configuration Tool or use the command line data import tool, **ldif2db**, as follows:

```
ldif2db -i replication.topology.ldif
```

After the replication topology entries are loaded, start the replica server and resume replication. You can resume replication in one of the following ways:

- On the master server, use **Manage Queues in Replication Management** in the Web Administration Tool.
- Use the new **ldapexop** command line utility. For example:

  ```
  ldapexop -h master-server-host-name -p master-server-port \
   -D master-server-admin-DN -w master-server-admin-password \
   -op controlrepl -action resume -ra replica-agreement-DN
  ```

  This command resumes replication for the server defined in the entry with the specified DN.

To determine which replica agreement DN corresponds to a replica server, look in the replication.topology.ldif file. The master server will log a message that replication has started for that replica and a warning that the replica server's ID in the agreement does not match the replica's server ID. To update the replica agreement to use the correct server ID, use **Replication Management** in the Web Administration Tool, or the command line tool **ldapmodify**. For example:

```
ldapmodify -c -h master-server-host-name -p master-server-port \
 -D master-server-admin-DN -w master-server-admin-password
dn: replica-agreement-DN
changetype: modify
replace: ibm-replicaConsumerID
ibm-replicaConsumerID: replica-server-ID
<empty line>
Ctrl+C
```

The empty line serves as a separator between entries. You can enter these commands directly on the command line, or you can save the commands in an LDIF file and supply them to the command with the **-i** *file* option.

Migration for this replica is complete.

To continue to use a replica running a previous version, it is still necessary to resume replication using the command line tool **ldapexop** or **Replication Management** in the Web Administration Tool for that replica. If a replica running a

previous version is migrated later, use the new command line tool **ldapdiff** to synchronize the directory data. This will ensure that entries or attributes that were not replicated are updated on the replica.

See the *IBM Directory Server version 5.1 Administration Guide* for information about using **ldapdiff**, **ldapexop**, and the Web Administration Tool.

Migrating a peer-master configuration

To migrate a configuration using peer masters, migrate each of the peers and replicas. As each peer master is started, part of the replication topology will be generated. To generate a complete replication topology, first perform the following search on each of the peer servers except for one.

```
ldapsearch -L -h peer-server-host-name -p peer-server-port \
 -D peer-admin-DN -w peer-admin-password \
 -b suffix-entry-DN
"(|(objectclass=ibm-replicaSubEntry)(objectclass=ibm-replicationAgreement))" \
  >> peer.topology.ldif
```

Use the output file created by searching all of the peers except one to complete the topology on the server that was not searched by adding the data from the command line. For example:

```
ldapadd -h peer-server-host-name -p peer-server-port \
 -D master-DN -w master-password \
 -c -i peer.topology.ldif
```

Use the master DN and password from this server's configuration file (/etc/ibmslapd.conf on UNIX or %LDAPHome%\etc\ibmslapd.conf on Windows). These were migrated from the previous version's peer DN and password. This will ensure that the added data is not replicated to servers that already contain these entries. The replication topology is now complete on this server, which can be used with the **ldapdiff** tool to synchronize the other peer masters. For example:

```
ldapdiff -b ibm-replicaGroup=default,suffix-entry-DN \
 -sh fixed-server-host-name -sD fixed-server-admin-DN -sw
fixed-server-admin-password \
 -ch peer-server-host-name -cD peer-server-admin-DN -cw
peer-server-admin-password \
 -F -a -v
```

Repeat these steps for each suffix entry that is to be replicated.

Replication can be resumed on each peer master to the other peer masters using either the Web Administration Tool or the command line tool **ldapexop** as described in "Migrating a single master configuration" on page 93. Each peer master has replica agreements for the other peer masters.

To complete the migration, export the replication topology entries as described in "Migrating a single master configuration" on page 93. Use the command line tool **ldapsearch** and save the output to a file. The search command is similar to the following:

```
ldapsearch -h peer-server-host-name -p peer-server-port \
 -D peer-server-admin-DN -w peer-server-admin-password \
 -b ibm-replicagroup=default,suffix-entry-DN \
 -L "(|(objectclass=ibm-replicaSubEntry)(objectclass=ibm-replicationAgreement))" \
     > replication.topology.ldif
```

This command will create an output LDIF file named replication.topology.ldif in the current working directory. The file will contain the complete replication topology. Import this file to the replicas that have been migrated as described in "Migrating a single master configuration" on page 93. Restart the replica server and resume replication for the migrated replica on each of the peer masters using the Web Administration Tool or **ldapexop**. For example, run the following command for each of the peer master servers:

```
ldapexop -h peer-server-host-name -p peer-server-port \
 -D peer-server-admin-DN -w peer-server-admin-password \
 -op controlrepl -action resume  -ra replica-agreement-DN
```

To update the replica agreement to use the correct server ID, use **Replication Management** in the Web Administration Tool , or the command line tool **ldapmodify**. For example:

```
ldapmodify -c -h peer-server-host-name -p peer-server-port \
 -D peer-server-admin-DN -w peer-server-admin-password
dn: replica-agreement-DN-on-peer-1
changetype: modify
replace: ibm-replicaConsumerID
ibm-replicaConsumerID: replica-server-ID
<empty line>
...
dn: replica-agreement-DN-on-peer-N
changetype: modify
replace: ibm-replicaConsumerID
ibm-replicaConsumerID: replica-server-ID
<empty line>
Ctrl+C
```

The empty lines serve as separators between entries.

You can enter these commands directly on the command line, or you can save the commands in an LDIF file and supply them to the command with the **-i***file* option.

The peer master will replicate these changes to each of the other peers. There should be a replica agreement for each peer master for this replica.

See the *IBM Directory Server version 5.1 Administration Guide* for information about using **ldapdiff**, **ldapexop**, and the Web Administration Tool.

Appendix D. Installing, configuring, and uninstalling embedded version of WebSphere Application Server - Express, V5.0

An application server is required to use the Web Administration Tool. The embedded version of WebSphere Application Server - Express, V5.0 is provided with IBM Directory Server 5.1 as an application server.

- If you use the InstallShield GUI with the Typical installation option to install the Web Administration Tool, and you do not have the embedded version of WebSphere Application Server - Express, V5.0 installed, the InstallShield GUI installs and configures the embedded version of WebSphere Application Server - Express, V5.0 automatically.
- If you use the InstallShield GUI with the Custom installation option to install the Web Administration Tool, you can select the embedded version of WebSphere Application Server - Express, V5.0 for installation. In this case, configuration is also done automatically.

If you use native installation methods, you can install and configure the embedded version of WebSphere Application Server - Express, V5.0 manually. If you already have the embedded version of WebSphere Application Server - Express, V5.0 installed, you must configure manually before you can use the Web Administration Tool.

Note: The embedded version of WebSphere Application Server - Express, V5.0 is not available for HP-UX. To use the Web Administration Tool on HP-UX, you must install an application server such as Apache Tomcat.

To manually install the embedded version of WebSphere Application Server - Express, V5.0 on UNIX platforms, do the following:

1. After you download and unzip (or untar) the IBM Directory Server zip or tar file, change directories to the directory where you expanded the file.
2. Type the following command at a command prompt:
   - On Windows platforms:

     ```
     install.bat -installRoot installpath\appsrv -hostName localhost
     ```

   - On UNIX platforms:

     ```
     install.sh -installRoot installpath/appsrv -hostName localhost
     ```

   where
   - *installpath* is the directory where you will install the Web Administration Tool.
   - *installpath/appsrv* is the directory where you will install the embedded version of WebSphere Application Server - Express, V5.0.

After installing the Web Administration Tool, copy the Web Administration Tool to the embedded version of WebSphere Application Server - Express, V5.0 directory by using the following commands:

```
mkdir installpath/appsrv/installableApps/
cp installpath/idstools/IDSWebApp.war installpath/appsrv/installableApps/
```

You can install and configure the Web Administration Tool into the embedded version of WebSphere Application Server - Express, V5.0 directory by using the following command:

```
installpath/appsrv/bin/wsadmin.sh -conntype NONE -c "\$AdminApp
     install {installpath/appsrv/installableApps/IDSWebApp.war}
     {-configroot \"installpath/appsrv/config\"
     -node DefaultNode -usedefaultbindings -nodeployejb -appname IDSWebApp.war
     -contextroot \"IDSWebApp\"}"
```

Note: If you install the Web Administration Tool and the embedded version of WebSphere Application Server - Express, V5.0 through the Installshield GUI, these commands are run automatically.

Uninstalling the Web Administration Tool from embedded version of WebSphere Application Server - Express, V5.0

To uninstall the Web Administration Tool from the embedded version of WebSphere Application Server - Express, V5.0 manually:

1. Be sure that the application server is started. See "Starting the application server to use the Web Administration Tool" on page 75 for instructions.
2. Type the following at a command prompt:
   - On Windows platforms:

     ```
     installpath\appsrv\bin\wsadmin.bat
     ```

   - On UNIX platforms:

     ```
     installpath/appsrv/bin/wsadmin.sh
     ```

     You are now in interactive mode, and messages are displayed.
3. At the wsadmin> prompt, type the following:

   ```
   $AdminApp uninstall IDSWebApp.war
   ```

   Messages are displayed.
4. At the wsadmin> prompt, type the following:

   ```
   $AdminConfig save
   quit
   ```

Appendix E. Installing and configuring DSML

DSML is installed as a .zip file named DSML.zip in the *installpath*/idstools (or *installpath*\idstools for Windows systems) when you install the Web Administration Tool. When you unzip the DSML.zip file, there are documentation files that tell you how to install, configure, and use DSML. The files are:

DSMLReadme.txt
: Describes the files in the package and tells you how to install and configure DSML.

dsml.pdf
: Describes how to use DSML. This file is in PDF format.

dsml.htm
: Describes how to use DSML, in HTML format.

Appendix F. UTF-8 support

IBM Directory supports a wide variety of national language characters through the UTF-8 (UCS Transformation Format) character set. As specified for the LDAP Version 3 protocol, all character data that is passed between an LDAP client and a server is in UTF-8. Consequently, the directory server can be configured to store any national language characters that can be represented in UTF-8. The limitations on what types of characters can be stored and searched for are determined by how the database is created. The database character set can be specified as UTF-8 or it can be allowed set to use the server system's local character set (based on the locale, language, and code page environment).

If you specify UTF-8, you can store any UTF-8 character data in the directory. LDAP clients running anywhere in the world (in any UTF-8 supported language) can access and search the directory. In many cases, however, the client has limited ability to properly display the results retrieved from the directory in a particular language/character set. There is also a performance advantage to using a UTF-8 database because no data conversion is required when storing data to or retrieving data from the database.

Why choose anything other than UTF-8?

A UTF-8 database has a fixed collation sequence. That sequence is the binary order of the UTF-8 characters. It is not possible to do language-sensitive collation with a UTF-8 database.

If it is important to your LDAP applications or users to get results for a search using an ordering filter (for example, "name >= SMITH") or any search specifying the control to sort the results, as they would expect for their native language, then UTF-8 might not be the appropriate character set for their directory database. In that instance, the LDAP server system and all client systems should run using the same character set and locale. For example, an LDAP server running in a Spanish locale with a database created using that locale returns results of searches based on character ordering, as Spanish-language clients would expect. This configuration does limit your directory user community to a single end-user character set and collation sequence.

Server utilities

Manual creation of an LDIF file containing UTF-8 values is difficult. To simplify this process, a charset extension to the LDIF format is supported. This extension allows an IANA character set name to be specified in the header of the LDIF file (along with the version number). A limited set of the IANA character sets are supported.

Examples

You can use the optional charset tag so that the server utilities automatically convert from the specified character set to UTF-8 as in the following example:

```
version: 1
charset: ISO-8859-1

dn: cn=Juan Griego, o=University of New Mexico, c=US
cn: Juan Griego
```

```
sn: Griego
description:: V2hhdCBhIGNhcmVmdWwgcmVhZGVyIHlvd
title: Associate Dean
title: [title in Spanish]
jpegPhoto:< file:///usr/local/photos/jgriego.jpg
```

In this instance, all values following an attribute name and a single colon are translated from the ISO-8859-1 character set to UTF-8. Values following an attribute name and a double colon (such as description:: V2hhdCBhIGNhcm...) should be base 64-encoded, and are expected to be either binary or UTF-8 character strings. Values read from a file, such as the jpegPhoto attribute specified by the URL in the example above, are also expected to be either binary or UTF-8. No translation from the specified ″charset″ to UTF-8 is done on those values.

In this example of an LDIF file without the charset tag, content is expected to be in UTF-8:

```
# IBM IBM Directorysample LDIF file
#
# The suffix "o=IBM, c=US" should be defined before attempting to load
# this data.

 version: 1

 dn: o=IBM, c=US
 objectclass: top
 objectclass: organization
 o: IBM

 dn: ou=Austin, o=IBM, c=US
 ou: Austin
 objectclass: organizationalUnit
 seealso: cn=Linda Carlesberg, ou=Austin, o=IBM, c=US
```

This same file could be used without the version: 1 header information, as in previous releases of the IBM Directory:

```
# IBM IBM Directorysample LDIF file
#
#The suffix "o=IBM, c=US" should be defined before attempting to load
#this data.

 dn: o=IBM, c=US
 objectclass: top
 objectclass: organization
 o: IBM

 dn: ou=Austin, o=IBM, c=US
 ou: Austin
 objectclass: organizationalUnit
 seealso: cn=Linda Carlesberg, ou=Austin, o=IBM, c=US
```

Supported IANA character sets

The IBM Directory supports the Internet Assigned Number Authority (IANA) character set names by platform, as shown in the following table. These are the character set names that can be specified in an LDIF file or via the C-client interface to identify the character set of input data to be used with the directory.

Table 3. Supported IANA character sets by platform

Character	Locale				DB2 Code Page	
Set Name	**Linux, Linux_390, HP-UX**	**NT**	**AIX**	**Solaris**	**UNIX**	**NT**
ISO-8859-1	X	X	X	X	819	1252
ISO-8859-2	X	X	X	X	912	1250
ISO-8859-5	X	X	X	X	915	1251
ISO-8859-6	X	X	X	n/a	1089	1256
ISO-8859-7	X	X	X	n/a	813	1253
ISO-8859-8	X	X	X	n/a	916	1255
ISO-8859-9	X	X	X	n/a	920	1254
IBM437	n/a	X	n/a	n/a	437	437
IBM850	n/a	X	X	n/a	850	850
IBM852	n/a	X	n/a	n/a	852	852
IBM857	n/a	X	n/a	n/a	857	857
IBM862	n/a	X	n/a	n/a	862	862
IBM864	n/a	X	n/a	n/a	864	864
IBM866	n/a	X	n/a	n/a	866	866
IBM869	n/a	X	n/a	n/a	869	869
TIS-620	n/a	X	X	n/a	874	874
EUC-JP	X	n/a	X	X	954	n/a
EUC-KR	n/a	n/a	X	X	970	n/a
EUC-CN	n/a	n/a	X	X	1383	n/a
EUC-TW	n/a	n/a	X	X	964	n/a
Shift-JIS	X	X	X	X	932	943
KSC	n/a	X	n/a	n/a	n/a	949
GBK	n/a	X	X	n/a	1386	1386
Big5	n/a	X	X	X	950	950

Appendix G. Setting up GSKit to support CMS key databases

To set up GSKit to support CMS key databases, do the following before starting the iKeyman GUI:

1. Install IBM or an IBM-equivalent JDK 1.3.
2. Set JAVA_HOME to point to the directory where JDK 1.3 was installed. For example:
   - On Windows, set JAVA_HOME=c:\Progam Files\IBM\Java13.
   - On AIX, export JAVA_HOME=/usr/opt/IBMJava2-13 for AIX.
3. Remove the gskikm.jar and ibmjcaprovider.jar files from your JAVA_HOME\jre\lib\ext directory.
4. Be sure that JAVA_HOME\jre\lib\ext\ has the following jar files:
   - ibmjceprovider.jar
   - ibmpkcs.jar
   - ibmjcefw.jar
   - local_policy.jar
   - US_export_policy.jar
   - ibmjlog.jar

   Note: GSKit has shipped these jar files and ibmjsse.jar under *GSKit Installation path*\classes\jre\lib\ext for your convenience. It is up to each individual product to decide whether they want to ship these JSSE jar files in their products. The following are GSKit recommendations:
   - A product should ship whatever JSSE jar files it used for system testing with the product.
   - If your existing Java 1.3 installation's JSSE jar files are later than those required by GSKit, no action is required.
   - If your existing Java 1.3 installation's JSSE jar files are older than those required by GSKit, your should replace your old JSSE jar files with the GSKit jar files. GSKit iKeyman will work with the old JSSE jar files.

     However, some iKeyman functions may fail due to known bug fixes that are not included in your JDK installation.
5. This step is optional. If you are a JSSE user and use JSSE to access crypto hardware, install the ibmjsse.jar in the JAVA_HOME\jre\lib\ext directory and follow the instructions in *GSKit Installation path*/classes/native/nativesupport.zip to setup the crypto hardware DLLs.
6. Register IBM JCE or IBM CMS service providers:
   - JSSE users need to register the IBMJCE provider as described below:

     Update the JAVA_HOME/jre/lib/security/java.security file to add the IBMJCE provider after the Sun provider. For example:
     - security.provider.1=sun.security.provider.Sun
     - security.provider.2=com.ibm.crypto.provider.IBM JCE

     A sample java.security file for JSSE user can be found in *GSKit Installation path*\classes\jsse_java.security.
   - GSKit users need to register both IBM CMS and IBM JCE service providers as described below:

Update the JAVA_HOME/jre/lib/security/java.security file to add both IBM CMS and IBM JCE providers after the Sun provider. For example:

- security.provider.1=sun.security.provider.Sun
- security.provider.2=com.ibm.spi.IBMCMSProvider
- security.provider.3=com.ibm.crypto.provider.IBMJCE

A sample java.security file can be found in *GSKit Installation path*\classes\gsk_java.security.

Note: Key database files from gsk5ikm will still work.

Appendix H. IBM Directory Server configuration schema

This appendix describes the Directory Information Tree (DIT) and the attributes that are used to configure the ibmslapd.conf file. In previous releases the directory configuration settings were stored in a proprietary format in the configuration file. Starting with the Version 3.2 release, the directory settings are stored using the LDIF format in the configuration file.

The configuration file has been renamed from slapd32.conf to ibmslapd.conf in the 5.1 release. The schema used by the configuration file is also now available. Attribute types can be found in the v3.config.at file, and object classes are in the v3.config.oc file. Attributes can be modified using the **ldapmodify** command. See the *IBM Directory Server version 5.1 Administration Guide* for information about the **ldapmodify** command.

Directory Information Tree

cn=Configuration

- cn=Admin
- cn=Event Notification
- cn=Front End
- cn=Kerberos
- cn=Master Server
- cn=Referral
- cn=Schema
  - cn=IBM Directory
    - cn=Config Backends
      - cn=ConfigDB
    - cn=RDBM Backends
      - cn=Directory
      - cn=ChangeLog
    - cn=LDCF Backends
      - cn=SchemaDB
- cn=SSL
  - cn=CRL
- cn=Transaction

cn=Configuration

DN cn=Configuration

Description

This is the top-level entry in the configuration DIT. It holds data of global interest to the server, although in practice it also contains miscellaneous items. Every attribute in the this entry comes from the first section (global stanza) of ibmslapd.conf.

Number

1 (required)

Object Class
ibm-slapdTop

Mandatory Attributes

- cn
- ibm-slapdAdminDN
- ibm-slapdAdminPW
- ibm-slapdErrorLog
- ibm-slapdPort
- ibm-slapdPwEncryption
- ibm-slapdSizeLimit
- ibm-slapdSysLogLevel
- ibm-slapdTimeLimit
- objectClass

Optional Attributes

- ibm-slapdACLAccess
- ibm-slapdACIMechanism
- ibm-slapdConcurrentRW (Deprecated)
- ibm-slapdMaxPendingChangesDisplayed
- ibm-slapdServerId
- ibm-slapdSupportedWebAdmVersion
- ibm-slapdVersion

cn=Admin

DN cn=Admin, cn=Configuration

Description
Global configuration settings for IBM Admin Daemon

Number
1 (required)

Object Class
ibm-slapdAdmin

Mandatory Attributes

- cn
- ibm-slapdErrorLog
- ibm-slapdPort

Optional Attributes

- ibm-slapdSecurePort

cn=Event Notification

DN cn=Event Notification, cn=Configuration

Description
Global event notification settings for IBM Directory Server 5.1

Number
0 or 1 (optional; needed only if you want to enable event notification)

Object Class
ibm-slapdEventNotification

Mandatory Attributes

- cn
- ibm-slapdEnableEventNotification
- objectClass

Optional Attributes

- ibm-slapdMaxEventsPerConnection
- ibm-slapdMaxEventsTotal

cn=Front End

DN cn=Front End, cn=Configuration

Description
Global environment settings that the server applies at startup.

Number
0 or 1 (optional)

Object Class
ibm-slapdFrontEnd

Mandatory Attributes

- cn
- objectClass

Optional Attributes

- ibm-slapdACLCache
- ibm-slapdACLCacheSize
- ibm-slapdDB2CP
- ibm-slapdEntryCacheSize
- ibm-slapdFilterCacheBypassLimit
- ibm-slapdFilterCacheSize
- ibm-slapdPlugin
- ibm-slapdSetenv
- ibm-slapdIdleTimeOut

cn=Kerberos

DN cn=Kerberos, cn=Configuration

Description
Global Kerberos authentication settings for IBM Directory Server 5.1.

Number
0 or 1 (optional)

Object Class
ibm-slapdKerberos

Mandatory Attributes

- cn
- ibm-slapdKrbEnable
- ibm-slapdKrbRealm

- ibm-slapdKrbKeyTab
- ibm-slapdKrbIdentityMap
- ibm-slapdKrbAdminDN
- objectClass

Optional Attributes

- None

cn=Master Server

DN cn=Master Server, cn=Configuration

Description
When configuring a replica, this entry holds the bind credentials and referral URL of the master server.

Number
0 or 1 (optional)

Object Class
ibm-slapdReplication

Mandatory Attributes

- cn
- ibm-slapdMasterPW (Mandatory if not using Kerberos authentication.)

Optional Attributes

- ibm-slapdMasterDN
- ibm-slapdMasterPW (Optional if using Kerberos authentication.)
- ibm-slapdMasterReferral
- objectClass

cn=Referral

DN cn=Referral, cn=Configuration

Description
This entry contains all the referral entries from the first section (global stanza) of ibmslapd.conf. If there are no referrals (there are none by default), this entry is optional.

Number
0 or 1 (optional)

Object Class
ibm-slapdReferral

Mandatory Attributes

- cn
- ibm-slapdReferral
- objectClass

Optional Attributes

- None

cn=Schemas

DN cn=Schemas, cn=Configuration

Description
This entry serves as a container for the schemas. This entry is not really necessary because the schemas can be distinguished by the object class ibm-slapdSchema. It is included to improve the readability of the DIT.

Only one schema entry is currently allowed: cn=IBM Directory.

Number
1 (required)

Object Class
Container

Mandatory Attributes
- cn
- objectClass

Optional Attributes
- None

cn=IBM Directory

DN cn=IBM Directory, cn=Schemas, cn=Configuration

Description
This entry contains all the schema configuration data from the first section (global stanza) of ibmslapd.conf. It also serves as a container for all the backends which use the schema. Multiple schemas are not currently supported, but if they were, then there would be one ibm-slapdSchema entry per schema. Note that multiple schemas are assumed to be incompatible. Therefore, a backend can be associated with a single schema only.

Number
1 (required)

Object Class
ibm-slapdSchema

Mandatory Attributes
- cn
- ibm-slapdSchemaCheck
- ibm-slapdIncludeSchema
- objectClass

Optional Attributes
- ibm-slapdSchemaAdditions

cn=Config Backends

DN cn=Config Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Description
This entry serves as a container for the Config backends.

Number
1 (required)

Object Class
Container

Mandatory Attributes

- cn
- objectClass

Optional Attributes

None

cn=ConfigDB

DN cn=ConfigDB, cn=Config Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Description

Configuration backend for IBM Directory server configuration

Number

0 - n (optional)

Object Class

ibm-slapdConfigBackend

Mandatory Attributes

- ibm-slapdSuffix
- ibm-slapdPlugin

Optional Attributes

- ibm-slapdReadOnly

cn=RDBM Backends

DN cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Description

This entry serves as a container for the RDBM backends. It effectively replaces the database rdbm line from ibmslapd.conf by identifying all sub-entries as DB2 backends. This entry is not really necessary because the RDBM backends can be distinguished by object class ibm-slapdRdbmBackend. It is included to improve the readability of the DIT.

Number

0 or 1 (optional)

Object Class

Container

Mandatory Attributes

- cn
- objectClass

Optional Attributes

- None

cn=Directory

DN cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Description

This entry contains all the database configuration settings for the default RDBM database backend.

Although multiple backends with arbitrary names can be created, the Server Administration assumes that ″cn=Directory″ is the main directory backend, and that ″cn=Change Log″ is the optional changelog backend. Only the suffixes displayed in ″cn=Directory″ are configurable through the Server Administration (except for the changelog suffix, which is set transparently by enabling changelog).

Number
0 - n (optional)

Object Class
ibm-slapdRdbmBackend

Mandatory Attributes

- cn
- ibm-slapdDbInstance
- ibm-slapdDbName
- ibm-slapdDbUserID
- objectClass

Optional Attributes

- ibm-slapdBulkloadErrors
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdDBAlias
- ibm-slapdDB2CP
- ibm-slapdDbConnections
- ibm-slapdDbLocation
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt
- ibm-slapdPageSizeLmt
- ibm-slapdPlugin
- ibm-slapdReadOnly
- ibm-slapdReplDbConns
- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSuffix
- ibm-slapdUseProcessIdPw

Note: If you are using **ibm-slapdUseProcessIdPw**, you must modify the schema to make **ibm-slapdDbUserPW** optional.

cn=Change Log

DN cn=Change Log, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Description
This entry contains all the database configuration settings for the change log backend.

Number
0 - n (optional)

Object Class
ibm-slapdRdbmBackend

Mandatory Attributes

- cn
- ibm-slapdDbInstance
- ibm-slapdDbName
- ibm-slapdDbUserID
- objectClass

Optional Attributes

- ibm-slapdBulkloadErrors
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdDBAlias
- ibm-slapdDB2CP
- ibm-slapdDbConnections
- ibm-slapdDbLocation
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt
- ibm-slapdPageSizeLmt
- ibm-slapdPlugin
- ibm-slapdReadOnly
- ibm-slapdReplDbConns
- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSuffix
- ibm-slapdUseProcessIdPw

Note: If you are using **ibm-slapdUseProcessIdPw**, you must modify the schema to make **ibm-slapdDbUserPW** optional.

cn=LDCF Backends

DN cn=LDCF Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Description
This entry serves as a container for the LDCF backends. It effectively replaces the database ldcf line from ibmslapd.conf by identifying all sub-entries as LDCF backends. This entry is not really necessary because the LDCF backends can be distinguished by the object class ibm-slapdLdcfBackend. It is included to improve the readability of the DIT.

Number
1 (required)

Object Class
Container

Mandatory Attributes

- cn
- objectClass

Optional Attributes

- ibm-slapdPlugin

cn=SchemaDB

DN cn=SchemaDB, cn=LDCF Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Description
This entry contains all the database configuration data from the ldcf database section of ibmslapd.conf.

Number
1 (required)

Object Class
ibm-slapdLdcfBackend

Mandatory Attributes

- cn
- objectClass

Optional Attributes

- ibm-slapdPlugin
- ibm-slapdSuffix

cn=SSL

DN cn=SSL, cn=Configuration

Description
Global SSL connection settings for IBM Directory Server 5.1.

Number
0 or 1 (optional)

Object Class
ibm-slapdSSL

Mandatory Attributes

- cn
- ibm-slapdSecurity
- ibm-slapdSecurePort
- ibm-slapdSslAuth
- objectClass

Optional Attributes

- ibm-slapdSslCertificate
- ibm-slapdSslCipherSpec

  Note: **ibm-slapdSslCipherSpecs** is now deprecated. Use **ibm-slapdSslCipherSpec** instead. If you use **ibm-slapdSslCipherSpecs**, the server will convert to the supported attribute.
- ibm-slapdSslKeyDatabase
- ibm-slapdSslKeyDatabasePW

cn=CRL

DN cn=CRL, cn=SSL, cn=Configuration

Description

This entry contains certificate revocation list data from the first section (global stanza) of ibmslapd.conf. It is only needed if ″ibm-slapdSslAuth = serverclientauth″ in the cn=SSL entry and the client certificates have been issued for CRL validation.

Number

0 or 1 (optional)

Object Class

ibm-slapdCRL

Mandatory Attributes

- cn
- ibm-slapdLdapCrlHost
- ibm-slapdLdapCrlPort
- objectClass

Optional Attributes

- ibm-slapdLdapCrlUser
- ibm-slapdLdapCrlPassword

cn=Transaction

DN cn = Transaction, cn = Configuration

Description

Specifies Global transaction support settings. Transaction support is provided using the plugin:

Windows 2000, or Windows NT operating system:

```
extendedop /bin/libtranext.dll tranExtOpInit 1.3.18.0.2.12.5
1.3.18.0.2.12.6
```

AIX:

```
extendedop /lib/libtranext.a tranExtOpInit 1.3.18.0.2.12.5
1.3.18.0.2.12.6
```

Solaris operating system:

```
extendedop /lib/libtranext.so tranExtOpInit 1.3.18.0.2.12.5
1.3.18.0.2.12.6
```

The server (**slapd**) loads this plugin automatically at startup if **ibm-slapdTransactionEnable = TRUE**. The plugin does not need to be explicitly added to **ibmslapd.conf**.

Number

0 or 1 (optional; required only if you want to use transactions.)

Object Class

ibm-slapdTransaction

Mandatory Attributes

- cn
- ibm-slapdMaxNumOfTransactions

- ibm-slapdMaxOpPerTransaction
- ibm-slapdMaxTimeLimitOfTransactions
- ibm-slapdTransactionEnable
- objectClass

Optional Attributes

- None

Attributes

- cn
- ibm-slapdACIMechanism
- ibm-slapdACLAccess
- ibm-slapdACLCache
- ibm-slapdACLCacheSize
- ibm-slapdAdminDN
- ibm-slapdAdminPW
- ibm-slapdBulkloadErrors
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdConcurrentRW
- ibm-slapdDB2CP
- ibm-slapdDBAlias
- ibm-slapdDbConnections
- ibm-slapdDbInstance
- ibm-slapdDbLocation
- ibm-slapdDbName
- ibm-slapdDbUserID
- ibm-slapdDbUserPW
- ibm-slapdEnableEventNotification
- ibm-slapdEntryCacheSize
- ibm-slapdErrorLog
- ibm-slapdFilterCacheBypassLimit
- ibm-slapdFilterCacheSize
- ibm-slapdIdleTimeOut
- ibm-slapdIncludeSchema
- ibm-slapdKrbAdminDN
- ibm-slapdKrbEnable
- ibm-slapdKrbIdentityMap
- ibm-slapdKrbKeyTab
- ibm-slapdKrbRealm
- ibm-slapdLdapCrlHost
- ibm-slapdLdapCrlPassword
- ibm-slapdLdapCrlPort
- ibm-slapdLdapCrlUser
- ibm-slapdMasterDN
- ibm-slapdMasterPW

- ibm-slapdMasterReferral
- ibm-slapdMaxEventsPerConnection
- ibm-slapdMaxEventsTotal
- ibm-slapdMaxNumOfTransactions
- ibm-slapdMaxOpPerTransaction
- ibm-slapdMaxPendingChangesDisplayed
- ibm-slapdMaxTimeLimitOfTransactions
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt
- ibm-slapdPageSizeLmt
- ibm-slapdPlugin
- ibm-slapdPort
- ibm-slapdPwEncryption
- ibm-slapdReadOnly
- ibm-slapdReferral
- ibm-slapdReplDbConns
- ibm-slapdReplicaSubtree
- ibm-slapdSchemaAdditions
- ibm-slapdSchemaCheck
- ibm-slapdSecurePort
- ibm-slapdSecurity
- ibm-slapdServerId
- ibm-slapdSetenv
- ibm-slapdSizeLimit
- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSslAuth
- ibm-slapdSslCertificate
- ibm-slapdSslCipherSpec
- ibm-slapdSslKeyDatabase
- ibm-slapdSslKeyDatabasePW
- ibm-slapdSslKeyRingFile
- ibm-slapdSuffix
- ibm-slapdSupportedWebAdmVersion
- ibm-slapdSysLogLevel
- ibm-slapdTimeLimit
- ibm-slapdTransactionEnable
- ibm-slapdUseProcessIdPw
- ibm-slapdVersion
- objectClass

cn

Description

This is the X.500 common Name attribute, which contains a name of an object.

Syntax
Directory string

Maximum Length
256

Value Multi-valued

ibm-slapdACIMechanism

Description
Determines which ACL model the server uses. (Supported only on OS/400® as of v3.2, ignored on other platforms.)

- 1.3.18.0.2.26.1 = IBM SecureWay v3.1 ACL model
- 1.3.18.0.2.26.2 = IBM SecureWay v3.2 ACL model

Default
1.3.18.0.2.26.2 = IBM SecureWay v3.2 ACL model

Syntax
Directory string

Maximum Length
256

Value Multi-valued.

ibm-slapdACLAccess

Description
Controls whether access to ACLs is enabled. If set to TRUE, access to ACLs is enabled. If set to FALSE, access to ACLs is disabled.

Default
TRUE

Syntax
Boolean

Maximum Length
5

Value Single-valued

ibm-slapdACLCache

Description
Controls whether or not the server caches ACL information.

- If set to TRUE, the server caches ACL information.
- If set to FALSE, the server does not cache ACL information.

Default
TRUE

Syntax
Boolean

Maximum Length
5

Value Single-valued

ibm-slapdACLCacheSize

Description
Maximum number of entries to keep in the ACL Cache.

Default
25000

Syntax
Integer

Maximum Length
11

Value Single-valued

ibm-slapdAdminDN

Description
The administrator bind DN for IBM Directory Server server.

Default
cn=root

Syntax
DN

Maximum Length
Unlimited

Value Single-valued

ibm-slapdAdminPW

Description
The administrator bind Password for IBM Directory Server server.

Default
secret

Syntax
Binary

Maximum Length
128

Value Single-valued

ibm-slapdBulkloadErrors

Description
File path or device on ibmslapd host machine to which bulkload error messages will be written. On Windows, forward slashes are allowed, and a leading slash not preceded by a drive letter is assumed to be rooted at the install directory (for example, /tmp/bulkload.errors = D:\Program Files\IBM\ldap\tmp\bulkload.errors).

Default
/var/bulkload.log

Syntax
Directory string with case-exact matching

Maximum Length
1024

Value Single-valued

ibm-slapdChangeLogMaxEntries

Description
This attribute is used by a changelog plug-in to specify the maximum number of changelog entries allowed in the RDBM database. Each changelog has its own changeLogMaxEntries attribute.

```
Minimum = 0 (unlimited)
Maximum = 2,147,483,647 (32-bit, signed integer)
```

Default
0

Syntax
Integer

Maximum Length
11

Value Single-valued

ibm-slapdCLIErrors

Description
File path or device on ibmslapd host machine to which CLI error messages will be written. On Windows, forward slashes are allowed, and a leading slash not preceded by a drive letter is assumed to be rooted at the install directory (for example, /tmp/cli.errors = D:\Program Files\IBM\ldap\tmp\cli.errors).

Default
/var/db2cli.log

Syntax
Directory string with case-exact matching

Maximum Length
1024

Value Single-valued

ibm-slapdConcurrentRW

Description
Setting this to TRUE allows searches to proceed simultaneously with updates. It allows for 'dirty reads', that is, results that might not be consistent with the committed state of the database.

Attention: This attribute is deprecated.

Default
FALSE

Syntax
Boolean

Maximum Length
5

Value Single-valued

ibm-slapdDB2CP

Description
Specifies the code page of the directory database. 1208 is the code page for UTF-8 databases.

Syntax
Directory string with case-exact matching

Maximum Length
11

Value Single-valued

ibm-slapdDBAlias

Description
The DB2 database alias.

Syntax
Directory string with case-exact matching

Maximum Length
8

Value Single-valued

ibm-slapdDbConnections

Description
Specify the number of DB2 connections the server will dedicate to the DB2 backend. The value must be between 5 & 50 (inclusive).

Note: ODBCCONS environment variable overrides the value of this directive.
If ibm-slapdDbConnections (or ODBCCONS) is less than 5 or greater than 50, the server will use 5 or 50 respectively. 1 additional connection will be created for replication (even if no replication is defined). 2 additional connections will be created for the change log (if change log is enabled).

Default
15

Syntax
Integer

Maximum Length
50

Value Single-valued

ibm-slapdDbInstance

Description
Specifies the DB2 database instance for this backend.

Default
ldapdb2

Syntax
Directory string with case-exact matching

Maximum Length
8

Value Single-valued

Note: All ibm-slapdRdbmBackend objects must use the same ibm-slapdDbInstance, ibm-slapdDbUserID, ibm-slapdDbUserPW and DB2 character set.

ibm-slapdDbLocation

Description
The file system path where the backend database is located. On UNIX, this is usually the home directory of the DB2 instance owner (for example, /home/ldapdb2). On Windows, it is a drive (for example, D:).

Syntax
Directory string with case-exact matching

Maximum Length
1024

Value Single-valued

ibm-slapdDbName

Description
Specifies the DB2 database name for this backend.

Default
ldapdb2

Syntax
Directory string with case-exact matching

Maximum Length
8

Value Single-valued

ibm-slapdDbUserID

Description
Specifies the user name with which to bind to the DB2 database for this backend.

Default
ldapdb2

Syntax
Directory string with case-exact matching

Maximum Length
8

Value Single-valued

Note: All ibm-slapdRdbmBackend objects must use the same ibm-slapdDbInstance ibm-slapdDbUserID, ibm-slapdDbUserPW and DB2 character set.

ibm-slapdDbUserPW

Description
Specifies the user password with which to bind to the DB2 database for this backend. The password can be plain text or imask encrypted.

Default
ldapdb2

Syntax
Binary

Maximum Length
128

Value Single-valued

Note: All ibm-slapdRdbmBackend objects must use the same ibm-slapdDbInstance, ibm-slapdDbUserID, ibm-slapdDbUserPW and DB2 character set.

ibm-slapdEnableEventNotification

Description
Specifies whether to enable Event Notification. It must be set to either TRUE or FALSE.

If set to FALSE, the server rejects all client requests to register event notifications with the extended result LDAP_UNWILLING_TO_PERFORM.

Default
TRUE

Syntax
Boolean

Maximum Length
5

Value Single-valued

ibm-slapdEntryCacheSize

Description
Maximum number of entries to keep in the entry cache.

Default
25000

Syntax
Integer

Maximum Length
11

Value Single-valued

ibm-slapdErrorLog

Description
Specifies the file path or device on the IBM Directory Server server machine to which error messages are written. On Windows 2000 or Windows NT operating systems, forward slashes are allowed, and a

leading slash not preceded by a drive letter is assumed to be rooted at the installation directory, that is /tmp/slapd.errors = c:\Program Files\IBM\ldap\var\ibmslapd.log.

Default
/var/ibmslapd.log

Syntax
Directory string with case-exact matching

Maximum Length
1024

Value Single-valued

ibm-slapdFilterCacheBypassLimit

Description
Search filters that match more than this number of entries will not be added to the Search Filter cache. Because the list of entry IDs that matched the filter are included in this cache, this setting helps to limit memory use. A value of 0 indicates no limit.

Default
100

Syntax
Integer

Maximum Length
11

Value Single-valued

ibm-slapdFilterCacheSize

Description
Specifies the maximum number of entries to keep in the Search Filter Cache.

Default
25000

Syntax
Integer

Maximum Length
11

Value Single-valued

ibm-slapdIdleTimeOut

Description
Maximum time to keep an LDAP connection open when there is no activity on the connection. The idle time for an LDAP connection is the time (in seconds) between the last activity on the connection and the current time. If the connection has expired, based on the idle time being greater than the value of this attribute, the LDAP server will clean up and end the LDAP connection, making it available for other incoming requests.

Default
300

Syntax
Integer

Length
11

Count Single

Usage Directory operation

User Modify
Yes

Access Class
Critical

Required
No

ibm-slapdIncludeSchema

Description
Specifies a file path on the IBM Directory Server server machine containing schema definitions. On Windows 2000, Windows NT, or Windows XP operating systems, forward slashes are allowed, and a leading slash not preceded by a drive letter (D:) is assumed to be rooted at the install directory, that is, /etc/V3.system.at = D:\Program Files\IBM\ldap\etc\V3.system.at.

Default
/etc/V3.system.at
/etc/V3.system.oc
/etc/V3.config.at
/etc/V3.config.oc
/etc/V3.ibm.at
/etc/V3.ibm.oc
/etc/V3.user.at
/etc/V3.user.oc
/etc/V3.ldapsyntaxes
/etc/V3.matchingrules

Syntax
Directory string with case-exact matching

Maximum Length
1024

Value Multi-valued

ibm-slapdKrbAdminDN

Description
Specifies the Kerberos ID of the LDAP administrator (for example, ibm-kn=admin1@realm1). Used when Kerberos authentication is used to authenticate the administrator when logged onto the Server Administration interface. This might be specified instead of or in addition to adminDN and adminPW.

Default
No preset default is defined.

Syntax
Directory string with case-exact matching

Maximum Length
128

Value Single-valued

ibm-slapdKrbEnable

Description
Specifies whether the server supports Kerberos authentication. It must be either TRUE or FALSE.

Default
TRUE

Syntax
Boolean

Maximum Length
5

Value Single-valued

ibm-slapdKrbIdentityMap

Description
Specifies whether to use Kerberos identity mapping. It must be set to either TRUE or FALSE. If set to TRUE, when a client is authenticated with a Kerberos ID, the server searches for all local users with matching Kerberos credentials, and adds those user DNs to the bind credentials of the connection. This allows ACLs based on LDAP user DNs to still be usable with Kerberos authentication.

Default
FALSE

Syntax
Boolean

Maximum Length
5

Value Single-valued

ibm-slapdKrbKeyTab

Description
Specifies the LDAP server Kerberos keytab file. This file contains the LDAP server private key, that is associated with its Kerberos account. This file is to be protected (like the server SSL key database file).

On Windows 2000, Windows NT, or Windows XP operating systems, forward slashes are allowed, and any path not preceded by a drive letter. (D:) is assumed to be rooted at the install directory (that is: /tmp/slapd.errors = D:\Program Files\IBM\ldap\tmp\slapd.errors).

Default
No preset default is defined.

Syntax
Directory string with case-exact matching

Maximum Length
1024

Value Single-valued

ibm-slapdKrbRealm

Description
Specifies the Kerberos realm of the LDAP server. It is used to publish the ldapservicename attribute in the root DSE. Note that an LDAP server can serve as the repository of account information for multiple KDCs (and realms), but the LDAP server, as a kerberized server, can only be a member of a single realm.

Default
No preset default is defined.

Syntax
Directory string with case-insensitive matching

Maximum Length
256

Value Single-valued

ibm-slapdLdapCrlHost

Description
Specifies the host name of the LDAP server that contains the Certificate Revocation Lists (CRLs) for validating client x.509v3 certificates. This parameter is needed when ibm-slapdSslAuth=serverclientauth and the client certificates have been issued for CRL validation.

Default
No preset default is defined.

Syntax
Directory string with case-insensitive matching

Maximum Length
256

Value Single-valued

ibm-slapdLdapCrlPassword

Description
Specifies the password that server-side SSL uses to bind to the LDAP server that contains the Certificate Revocation Lists (CRLs) for validating client x.509v3 certificates. This parameter might be needed when ibm-slapdSslAuth=serverclientauth and the client certificates have been issued for CRL validation.

Note: If the LDAP server holding the CRLs permits unauthenticated access to the CRLs (that is, anonymous access), then ibm-slapdLdapCrlPassword is not required.

Default
No preset default is defined.

Syntax
Binary

Maximum Length
128

Value Single-valued

ibm-slapdLdapCrlPort

Description
Specifies the port used to connect to the LDAP server that contains the Certificate Revocation Lists (CRLs) for validating client x.509v3 certificates. This parameter is needed when ibm-slapdSslAuth=serverclientauth and the client certificates have been issued for CRL validation. (IP ports are unsigned, 16-bit integers in the range 1 - 65535)

Default
No preset default is defined.

Syntax
Integer

Maximum Length
11

Value Single-valued

ibm-slapdLdapCrlUser

Description
Specifies the bindDN that the server-side SSL uses to bind to the LDAP server that contains the Certificate Revocation Lists (CRLs) for validating client x.509v3 certificates. This parameter might be needed when ibm-slapdSslAuth=serverclientauth and the client certificates have been issued for CRL validation.

Note: If the LDAP server holding the CRLs permits unauthenticated access to the CRLs (that is, anonymous access), then ibm-slapdLdapCrlUser is not required.

Default
No preset default is defined.

Syntax
DN

Maximum Length
1000

Value Single-valued

ibm-slapdMasterDN

Description
Specifies the bind DN of master server. The value must match the replicaBindDN in the replicaObject defined for the master server. When Kerberos is used to authenticate to the replica, ibm-slapdMasterDN must specify the DN representation of the Kerberos ID (for example, ibm-kn=freddy@realm1). When Kerberos is used, MasterServerPW is ignored.

Default
No preset default is defined.

Syntax
DN

Maximum Length
1000

Value Single-valued

ibm-slapdMasterPW

Description
Specifies the bind password of master replica server. The value must match replicaBindDN in the replicaObject defined for the master server. When Kerberos is used to authenticate to the replica, ibm-slapdMasterDN must specify the DN representation of the Kerberos ID (for example, ibm-kn=freddy@realm1). When Kerberos is used, MasterServerPW is ignored.

Default
No preset default is defined.

Syntax
Binary

Maximum Length
128

Value Single-valued

ibm-slapdMasterReferral

Description
Specifies the URL of the master replica server. For example:

```
ldap://master.us.ibm.com
```

For security set to SSL only:

```
ldaps://master.us.ibm.com:636
```

For security set to none and using a nonstandard port:

```
ldap://master.us.ibm.com:1389
```

Default
none

Syntax
Directory string with case-insensitive matching

Maximum Length
256

Value Single-valued

ibm-slapdMaxEventsPerConnection

Description
Specifies the maximum number of event notifications which can be registered per connection.

```
Minimum = 0 (unlimited)
Maximum = 2,147,483,647
```

Default
100

Syntax
Integer

Maximum Length
11

Value Single-valued

ibm-slapdMaxEventsTotal

Description
Specifies the maximum total number of event notifications which can be registered for all connections.

```
Minimum = 0 (unlimited)
Maximum = 2,147,483,647
```

Default
0

Syntax
Integer

Maximum Length
11

Value Single-valued

ibm-slapdMaxNumOfTransactions

Description
Specifies the maximum number of transactions per server.

```
Minimum = 0 (unlimited)
Maximum = 2,147,483,647
```

Default
20

Syntax
Integer

Maximum Length
11

Value Single-valued

ibm-slapdMaxOpPerTransaction

Description
Specifies the maximum number of operations per transaction.

```
Minimum = 0 (unlimited)
Maximum = 2,147,483,647
```

Default
5

Syntax
Integer

Maximum Length
11

Value Single-valued

ibm-slapdMaxPendingChangesDisplayed

Description
Maximum number of pending changes to be displayed.

Default
200

Syntax
Integer

Maximum Length
11

Value Single-valued

ibm-slapdMaxTimeLimitOfTransactions

Description
Specifies the maximum timeout value of a pending transaction in seconds.

```
Minimum = 0 (unlimited)
Maximum = 2,147,483,647
```

Default
300

Syntax
Integer

Maximum Length
11

Value Single-valued

ibm-slapdPagedResAllowNonAdmin

Description
Whether or not the server should allow non-Administrator bind for paged results requests on a search request. If the value read from the ibmslapd.conf file is FALSE, the server will process only those client requests submitted by a user with Administrator authority. If a client requests paged results for a search operation, does not have Administrator authority, and the value read from the ibmslapd.conf file for this attribute is FALSE, the server will return to the client with return code insufficientAccessRights; no searching or paging will be performed.

Default
FALSE

Syntax
Boolean

Length
5

Count Single

Usage directoryOperation

User Modify
Yes

Access Class
critical

Objectclass
ibm-slapdRdbmBackend

Required
No

ibm-slapdPagedResLmt

Description
Maximum number of outstanding paged results search requests allowed active simultaneously. Range = 0.... If a client requests a paged results operation, and a maximum number of outstanding paged results are currently active, then the server will return to the client with return code of busy; no searching or paging will be performed.

Default
3

Syntax
Integer

Length
11

Count Single

Usage directoryOperation

User Modify
Yes

Access Class
critical

Required
No

Objectclass
ibm-slapdRdbmBackend

ibm-slapdPageSizeLmt

Description
Maximum number of entries to return from search for an individual page when paged results control is specified, regardless of any pagesize that might have been specified on the client search request. Range = 0.... If a client has passed a page size, then the smaller value of the client value and the value read from ibmslapd.conf will be used.

Default
50

Syntax
Integer

Length
11

Count Single

Usage directoryOperation

User Modify
Yes

Access Class
critical

Required
No

Objectclass
ibm-slapdRdbmBackend

ibm-slapdPlugin

Description
A plugin is a dynamically loaded library which extends the capabilities of the server. An ibm-slapdPlugin attribute specifies to the server how to load and initialize a plug-in library. The syntax is:

```
keyword filename init_function [args...]
```

The syntax is slightly different for each platform because of library naming conventions. See the *Server Plug-ins Reference* for a list of plug-ins shipped with IBM Directory Server.

Most plug-ins are optional, but the RDBM backend plug-in is required for all RDBM backends.

Default
database /bin/libback-rdbm.dll rdbm_backend_init

Syntax
Directory string with case-exact matching

Maximum Length
2000

Value Multi-valued

ibm-slapdPort

Description
Specifies the TCP/IP port used for non-SSL connections. It cannot have the same value as ibm-slapdSecurePort. (IP ports are unsigned, 16-bit integers in the range 1 - 65535.)

Default
389

Syntax
Integer

Maximum Length
5

Value Single-valued

ibm-slapdPWEncryption

Description
Specifies the encoding mechanism for the user passwords before they are stored in the directory. It must be specified as none, imask, crypt, or sha (you must use the keyword **sha** in order to get SHA-1 encoding). The value must be set to none for the SASL cram-md5 bind to succeed.

Default
none

Syntax
Directory string with case-insensitive matching

Maximum Length
5

Value Single-valued

ibm-slapdReadOnly

Description
This attribute is normally applied to only the Directory backend. It specifies whether the backend can be written to. It must be specified as either TRUE or FALSE. It defaults to FALSE if unspecified. If set to TRUE, the server returns LDAP_UNWILLING_TO_PERFORM (0x35) in response to any client request which changes data in the readOnly database.

Default
FALSE

Syntax
Boolean

Maximum Length
5

Value Single-valued

ibm-slapdReferral

Description
Specifies the referral LDAP URL to pass back when the local suffixes do not match the request. It is used for superior referral (that is, the suffix is not within the naming context of the server).

Default
No preset default is defined.

Syntax
Directory string with case-exact matching

Maximum Length
32700

Value Multi-valued

ibm-slapdReplDbConns

Description
Maximum number of database connections for use by replication.

Default
4

Syntax
Integer

Maximum Length
11

Value Single-valued

ibm-slapdReplicaSubtree

Description
Identifies the DN of a replicated subtree

Syntax
DN

Maximum Length
1000

Value Single-valued

ibm-slapdSchemaAdditions

Description
The ibm-slapdSchemaAdditions attribute is used to identify explicitly which file holds new schema entries. This is set by default to be /etc/V3.modifiedschema. If this attribute is not defined, the server reverts to using the last ibm-slapdIncludeSchema file as in previous releases.

Before Version 3.2, the last includeSchema entry in **slapd.conf** was the file to which any new schema entries were added by the server if it received an add request from a client. Normally the last includeSchema is the V3.modifiedschema file, which is an empty file installed just for this purpose.

Note: The name modified is misleading, for it only stores new entries. Changes to existing schema entries are made in their original files.

Default
/etc/V3.modifiedschema

Syntax
Directory string with case-exact matching

Maximum Length
1024

Value Single-valued

ibm-slapdSchemaCheck

Description
Specifies the schema checking mechanism for the add/modify/delete operation. It must be specified as V2, V3, or V3_lenient.

- V2 - Retain v2 and v2.1 checking. Recommended for migration purpose.
- V3 - Perform v3 checking.
- V3_lenient - Not all parent object classes are needed. Only the immediate object class is needed when adding entries.

Default
V3_lenient

Syntax
Directory string with case-insensitive matching

Maximum Length
10

Value Single-valued

ibm-slapdSecurePort

Description
Specifies the TCP/IP port used for SSL connections. It cannot have the same value as ibm-slapdPort. (IP ports are unsigned, 16-bit integers in the range 1 - 65535.)

Default
636

Syntax
Integer

Maximum Length
5

Value Single-valued

ibm-slapdSecurity

Description
Enables SSL connections. Must be none, SSL, or SSLOnly.

- none - server listens on the non-ssl port only.
- SSL - server listens on both the ssl and the non-ssl ports.
- SSLOnly - server listens on the ssl port only.

Default
none

Syntax
Directory string with case-insensitive matching

Maximum Length
7

Value Single-valued

ibm-slapdServerId

Description
Identifies the server for use in replication.

Syntax
IA5 String with case-sensitive matching

Maximum Length
240

Value Single-valued

ibm-slapdSetenv

Description
The server runs **putenv()** for all values of ibm-slapdSetenv at startup to modify the server runtime environment. Shell variables (like %PATH% or $LANG) are not expanded.

Default
No preset default is defined.

Syntax
Directory string with case-exact matching

Maximum Length
2000

Value Multi-valued

ibm-slapdSizeLimit

Description
Specifies the maximum number of entries to return from search, regardless of any size limit that might have been specified on the client search request (Range = 0...). If a client has passed a limit, then the smaller value of the client values and the value read from **ibmslapd.conf** are used. If a client has not passed a limit and has bound as admin DN, the limit is considered unlimited. If the client has not passed a limit and has not bound as admin DN, then the limit is that which was read from the **ibmslapd.conf** file. 0 = unlimited.

Default
500

Syntax
Integer

Maximum Length
12

Value Single-valued

ibm-slapdSortKeyLimit

Description
The maximum number of sort conditions (keys) that can be specified on a single search request. Range = 0.... If a client has passed a search request with more sort keys than the limit allows, and the sorted search control criticality is FALSE, then the server will honor the value read from the ibmslapd.conf file and ignore any sort keys encountered after the limit has been reached - searching and sorting will be performed. If a client has passed a search a request with more keys than the limit allows, and the sorted search control criticality is TRUE, then the server will return to the client with a return code of **adminLimitExceeded** - no searching or sorting will be performed.

Default
3

Syntax
cis

Length
11

Count Single

Usage directoryOperation

User Modify
Yes

Access Class
critical

Objectclass
ibm-slapdRdbmBackend

Required
No

ibm-slapdSortSrchAllowNonAdmin

Description
Whether or not the server should allow non-Administrator bind for sort on a search request. If the value read from the ibmslapd.conf file is FALSE, the server will process only those client requests submitted by a user with Administrator authority. If a client requests sort for a search operation, does not have Administrator authority, and the value read from the ibmslapd.conf file for this attribute is FALSE, the server will return to the client with return code insufficientAccessRights - no searching or sorting will be performed.

Default
FALSE

Syntax
Boolean

Length
5

Count Single

Usage directoryOperation

User Modify
Yes

Access Class
critical

Objectclass
ibm-slapdRdbmBackend

Required
No

ibm-slapdSslAuth

Description
Specifies the authentication type for the ssl connection, either serverauth or serverclientauth.

- serverauth - supports server authentication at the client. This is the default.

- serverclientauth - supports both server and client authentication.

Default
serverauth

Syntax
Directory string with case-insensitive matching

Maximum Length
16

Value Single-valued

ibm-slapdSslCertificate

Description
Specifies the label that identifies the server Personal Certificate in the key database file. This label is specified when the server private key and certificate are created with the **gsk4ikm** application. If ibm-slapdSslCertificate is not defined, the default private key, as defined in the key database file, is used by the LDAP server for SSL connections.

Default
No preset default is defined.

Syntax
Directory string with case-exact matching

Maximum Length
128

Value Single-valued

ibm-slapdSslCipherSpec

Specifies the method of SSL encryption for clients accessing the server. Must be set to one of the following:

Table 4. Methods of SSL encryption

Attribute	Encryption level
TripleDES-168	Triple DES encryption with a 168-bit key and a SHA-1 MAC
DES-56	DES encryption with a 56-bit key and a SHA-1 MAC
RC4-128-SHA	RC4 encryption with a 128-bit key and a SHA-1 MAC
RC4-128-MD5	RC4 encryption with a 128-bit key and a MD5 MAC
RC2-40-MD5	RC4 encryption with a 40-bit key and a MD5 MAC
RC4-40-MD5	RC4 encryption with a 40-bit key and a MD5 MAC
AES	AES encryption

Syntax
IA5 String

Maximum Length
30

ibm-slapdSslKeyDatabase

Description

Specifies the file path to the LDAP server SSL key database file. This key database file is used for handling SSL connections from LDAP clients, as well as for creating secure SSL connections to replica LDAP servers.

On Windows 2000, Windows NT, or Windows XP operating systems, forward slashes are allowed, and a leading slash not preceded by a drive specifier (D:) is assumed to be rooted at the installation directory (that is, /etc/key.kdb = D:\Program Files\IBM\ldap\etc\key.kdb).

Default

/etc/key.kdb

Syntax

Directory string with case-exact matching

Maximum Length

1024

Value Single-valued

ibm-slapdSslKeyDatabasePW

Description

Specifies the password associated with the LDAP server SSL key database file, as specified on the ibm-slapdSslKeyDatabase parameter. If the LDAP server key database file has an associated password stash file, then the ibm-slapdSslKeyDatabasePW parameter can be omitted, or set to none.

Note: The password stash file must be located in the same directory as the key database file and it must have the same file name as the key database file, but with an extension of .sth instead of .kdb.

Default

none

Syntax

Binary

Maximum Length

128

Value Single-valued

ibm-slapdSslKeyRingFile

Description

Path to the LDAP server's SSL key database file. This key database file is used for handling SSL connections from LDAP clients, as well as for creating secure SSL connections to replica LDAP servers. On Windows, forward slashes are allowed, and a leading slash not preceded by a drive specifier is assumed to be rooted at the install directory (for example, /etc/key.kdb = c:\Program Files\IBM\ldap\etc\key.kdb).

Default

key.kdb

Syntax

Directory String with case-sensitive matching

Maximum Length
1024

Value Single-valued

ibm-slapdSuffix

Description
Specifies a naming context to be stored in this backend.

Note: This has the same name as the object class.

Default
No preset default is defined.

Syntax
DN

Maximum Length
1000

Value Multi-valued

ibm-slapdSupportedWebAdmVersion

Description
This attribute defines the earliest version of the Web Administration Tool that supports this server of cn=configuration.

Default

Syntax
Directory String

Maximum Length

Value Single-valued

ibm-slapdSysLogLevel

Description
Specifies the level at which debugging and operation statistics are logged in the slapd.errors file. It must be specified as l, m, or h.

- h - high (provides the most information)
- m - medium (the default)
- l - low (provides the least information)

Default
m

Syntax
Directory string with case-insensitive matching

Maximum Length
1

Value Single-valued

ibm-slapdTimeLimit

Description
Specifies the maximum number of seconds to spend on a search request,

regardless of any time limit that might have been specified on the client request. If a client has passed a limit, then the smaller value of the client values and the value read from **ibmslapd.conf** are used. If a client has not passed a limit and has bound as admin DN, the limit is considered unlimited. If the client has not passed a limit and has not bound as admin DN, then the limit is that which was read from the **ibmslapd.conf** file. 0 = unlimited.

Default
900

Syntax
Integer

Maximum Length

Value Single-valued

ibm-slapdTransactionEnable

Description
If the transaction plugin is loaded but ibm-slapdTransactionEnable is set to FALSE, the server rejects all StartTransaction requests with the response `LDAP_UNWILLING_TO_PERFORM`.

Default
TRUE

Syntax
Boolean

Maximum Length
5

Value Single-valued

ibm-slapdUseProcessIdPw

Description
If set to TRUE, the server ignores the ibm-slapdDbUserID and the ibm-slapdDbUserPW attributes and uses its own process credentials to authenticate to DB2.

Default
FALSE

Syntax
Boolean

Maximum Length
5

Value Single-valued

ibm-slapdVersion

Description
IBM Slapd version Number

Default

Syntax
Directory String with case-sensitive matching

Maximum Length

Value Single-valued

objectClass

Description

The values of the objectClass attribute describe the kind of object which an entry represents.

Syntax

Directory string

Maximum Length

128

Value Multi-valued

Appendix I. Notices

This information was developed for products and services offered in the U.S.A. IBM might not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the information. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this information at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Department LZKS
11400 Burnet Road
Austin, TX 78758
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, or other countries, or both:

AIX
AIX 5L
DB2
IBM
OS/400
RS/6000
SecureWay
SP
Tivoli
WebSphere

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation

UNIX is a registered trademark in the United States and/or other countries licensed exclusively through X/Open Company Limited.

Other company, product, and service names may be trademarks or service marks of others.

Index

J

K

L

M

N

O

P

R

S

T

U

V

W

Z

Printed in U.S.A.